	Балтийская государственная академия рыбопромыслового флота		
	Фонд оценочных средств для аттестации по дисциплине «Организационное и правовое обеспечение информационной безопасности»		
	Версия: 1	Дата выпуска версии: 15.05.18 г.	стр. 1 из 37

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)

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

(наименование дисциплины)

базовой 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.Б.29 «Организационное и правовое обеспечение информационной безопасности»

(код) (наименование дисциплины)

№ п/п	Контролируемые модули, разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Оценочные средства		Способ контроля
			наименование	№№ заданий	
1	РАЗДЕЛ 1. Законодательство РФ в области информационной безопасности	ОК-5 ОПК-6	собеседование, доклад	1.1	устный
			контрольная работа	Б	письменный
			защита лабораторного практикума	1.7	устный
				1.8	
				1.9	
				1.10	
				1.11	
2	РАЗДЕЛ 2. Правовые основы защиты государственной тайны	ОК-5 ОПК-6	собеседование, доклад	2.1	устный
			контрольная работа	Б	письменный
3	РАЗДЕЛ 3. Правовые основы защиты конфиденциальной информации	ОК-5 ОК-6 ОПК-6	коллоквиум, доклад	2.2 2.3	устный
			реферат, доклад	1, 2	письменный
4	РАЗДЕЛ 4. Правовое регулирование деятельности организаций в области информационной безопасности	ОК-5 ОК-6 ОПК-6 ПК-11 ПК-21	защита лабораторного практикума	1.7 1.8	устный
5	РАЗДЕЛ 5. Юридическая ответственность за правонарушения в области информационной безопасности	ОК-5 ОК-6 ОПК-6 ПК-11 ПК-20 ПК-23	собеседование, доклад	1.1	устный
			контрольная работа	Б	письменный
6	РАЗДЕЛ 6. Концептуальные положения организационного обеспечения информационной безопасности	ОК-5 ОК-6 ПК-11 ПК-21 ПК-22	защита лабораторного практикума	1.7 1.8 1.10	устный
			тестирование	А	письменный
7	РАЗДЕЛ 7. Организационная структура системы обеспечения информационной безопасности	ОК-5 ОПК-6 ПК-21 ПК-22 ПК-23	защита лабораторного практикума	1.7 1.8 1.10	устный
			контрольная работа	Б	письменный
8	РАЗДЕЛ 8. Организация и обеспечение режима секретности на объекте	ОК-5 ОК-6 ОПК-6 ПК-23	коллоквиум, доклад	1.2 1.3	устный
9	РАЗДЕЛ 9. Охрана объектов	ОК-5 ОК-6 ОПК-6 ПК-11	коллоквиум, доклад	1.2 1.3	устный
			контрольная	Б	письменный

			работа		

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.29 «Организационное и правовое обеспечение информационной безопасности»

(код) (наименование дисциплины)

№ п/п	Код компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студенты должны:		
			знать	уметь	владеть
1.	ОК-5	способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения ИБ и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности	роль и место информационной безопасности в системе национальной безопасности страны; основные термины по проблематике информационной безопасности	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	навыками формальной постановки и решения задачи обеспечения информационной безопасности автоматизированных систем
2.	ОК-6	способность к работе в коллективе, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность	теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию, основы правового регулирования взаимоотношений администрации и персонала в области защиты информации	самостоятельно получать знания для решения исследовательских задач, задач повышенной сложности	технологиями систематизации и накопления научных знаний в предметной области

3.	ОПК-6	способность применять нормативные правовые акты в профессиональной деятельности	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в автоматизированных системах	применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	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.	ПК-1	способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня (объектно-ориентированное программирование	применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации	навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках

5.	ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня	применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации	навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках
6.	ПК-20	способностью разрабатывать политики информационной безопасности автоматизированных систем	методы анализа и оценки угроз ИБ объектов информатизации, средства и методы физической защиты объектов, принципы построения систем защиты информации автоматизированных систем	выявлять уязвимости автоматизированных систем и ее системы защиты, определять необходимые и достаточные затрат на информационную безопасность предприятия	методами формирования требований по защите информации
7.	ПК-21	способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности

8.	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 информационной безопасности автоматизированных систем	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
9.	ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем	навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками организации и обеспечения режима секретности; навыками работы с технической документацией на ЭВМ и вычислительные системы

ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.29 «Организационное и правовое обеспечение информационной безопасности»

(код) (наименование дисциплины)

Семестр V

№ п/п	Код контролируемой компетенции (или ее части)	№ учебной недели																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		Этапы формирования компетенции																	
1.	ОК-5	+		+	+									+					
2.	ОК-6	+	+				+	+						+	+	+	+	+	
3.	ОПК-6	+		+	+			+	+				+	+					
4.	ПК-1					+					+	+					+	+	
5.	ПК-11					+						+	+	+					
6.	ПК-20		+		+	+	+		+						+	+		+	
7.	ПК-21									+	+	+			+				
8.	ПК-22									+	+	+				+	+	+	+
9.	ПК-23																+		+

ПОКАЗАТЕЛИ И КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ п/п	Код контролируемой компетенции (или ее части)	Уровни сформированности компетенции		
		пороговый	продвинутый	высокий
1	ОК-5	Знать:		
		средства и организационные меры обеспечения информационной безопасности	сущность и понятие информационной безопасности, характеристику ее составляющих	средства и организационные меры обеспечения информационной безопасности
		Уметь:		
		объяснить необходимость изучения информационной безопасности	самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять границы использования знаний	объяснить необходимость изучения информационной безопасности
		Владеть:		
		технологиями систематизации и накопления научных знаний в предметной области	методиками выполнения научно-исследовательских работ	технологиями систематизации и накопления научных знаний в предметной области
2	ОК-6	Знать:		
		требования к сотрудникам организации, допущенным к конфиденциальной информации	угрозы информации, средства и методы обеспечения информационной безопасности	требования к сотрудникам организации, допущенным к конфиденциальной информации
		Уметь:		
		применять действующую законодательную базу в области информационной безопасности	самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять границы использования знаний	применять действующую законодательную базу в области информационной безопасности
		Владеть:		
		технологиями систематизации и накопления научных знаний в предметной области	методиками выполнения научно-исследовательских работ	технологиями систематизации и накопления научных знаний в предметной области
3	ОПК-6	Знать:		
		понятие и виды защищаемой информации по законодательству РФ	правовые основы защиты информации с использованием технических средств	законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации
		Уметь:		
		отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законо-	применять действующую законодательную базу в области информационной безопасности	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положе-

		дательства, в том числе с помощью систем правовой информации		ний, инструкций и других организационных документов, анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития
		Владеть:		
		навыками разработки и использования нормативно-методическими материалами по регламентации системы организационной защиты информации	методиками выполнения научно-исследовательских работ	методологией прикладных научных исследований в предметной области
4	ПК-1	Знать:		
		классификацию и характеристики информационных баз и хранилищ	информационные базы и хранилища, порядок обращения к ним и поиска информации	порядок обработки патентной информации, информации по интеллектуальной собственности
		Уметь:		
		определить пути получения научно-технической информации, обобщать и систематизировать информацию	использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины	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
5	ПК-11	Знать:		
		уровни политики безопасности и ответственные за них, методы оценки рисков	теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию	методы анализа и оценки угроз ИБ объектов информатизации, средства и методы физической защиты объектов, принципы построения систем защиты информации автоматизированных систем
		Уметь:		
		отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития	выявлять уязвимости автоматизированных систем и ее системы защиты, определять необходимые и достаточные затрат на информационную безопасность предприятия
		Владеть:		
		методами формирования требований по защите информации	методиками выполнения научно-исследовательских работ	методологией прикладных научных исследований в предметной области
6	ПК-20	Знать:		
		автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	современные подходы к построению систем защиты информации в автоматизированных системах	нормативную базу эксплуатации и эксплуатационную документацию автоматизированных систем
		Уметь:		

		отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	применять действующую законодательную базу в области информационной безопасности	выбирать и анализировать эксплуатационные показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
		Владеть:		
		навыками разработки нормативно-методических материалов по регламентации организационной защиты информации	навыками работы с нормативно-правовыми актами	методологией прикладных научных исследований в предметной области
7	ПК-21	Знать:		
		направления создания правовой базы в области информационной безопасности	причины нарушения целостности информации	особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну
		Уметь:		
		пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов
		Владеть:		
		технологиями систематизации и накопления научных знаний в предметной области	методиками выполнения научно-исследовательских работ	методологией прикладных научных исследований в предметной области
8	ПК-22	Знать:		
		основные принципы, реализуемые при разработке политики информационной безопасности организации	основные виды политики информационной безопасности организации	основные этапы разработки концепции безопасности организации, содержание документов политики информационной безопасности
		Уметь:		
		разрабатывать функциональные обязанности должностных лиц организации по вопросам защиты информации	вносить необходимые изменения и дополнения в распорядительные документы по вопросам обеспечения информационной безопасности программно-информационных ресурсов	производить периодический анализ состояния и контроль эффективности реализуемых мер защиты информации
		Владеть:		
		навыками соблюдения правил защиты информации	навыками разработки концепции информационной безопасности организации (предприятия)	методикой управления инцидентами и мониторингом подсистемы информационной безопасности АС
9	ПК-23	Знать:		
		основные меры обеспечения информационной безопасности автоматизированной системы	основные мероприятия по защите информации от утечки по техническим каналам	основные мероприятия по пресечению несанкционированного доступа к конфиденциальной информации
		Уметь:		
		разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности автоматизированной системы организации	обеспечивать соблюдение соответствующего режима ограничения и разграничения доступа к информации, контроль выполнения установленных правил работы в	производить обобщенное описание объектов защиты, используя основные правила построения модели угроз и модели нарушителя, с дальнейшей реализацией принципов кон-

			автоматизированной системе	троля эффективности информационной безопасности автоматизированной системы
		Владеть:		
		навыками разработки концепции информационной безопасности организации (предприятия)	методикой управления инцидентами и мониторингом подсистемы информационной безопасности автоматизированной системы	навыками соблюдения правил защиты информации

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; - расширение проблематики в рамках дополнительных вопросов по данной 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, готовность принять позицию другого учащегося).	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 преподавателю необходимо 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 изложения мыслей, наличие и достаточность пояснений, культуру в предметной области.	Комплект контрольных заданий по вариантам
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	Образец рабочей тетради

	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.	
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. Доклады направлены на более глубокое самостоятельное изучение лекционного материала или рассмотрения вопросов для дополнительного изучения. 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
Экзамен	Экзамен проводится с целью проверки знаний и умений студентов по дисциплинам базовой части профессионального цикла. Основные задачи экзамена: оценивание теоретических знаний студентов по дисциплинам профессионального цикла; закрепление навыков глубокого, творческого и всестороннего анализа научной, методической и другой литературы по учебным дисциплинам; вырабатывание у студентов навыков и умений грамотно и убедительно излагать изученный учеб-	Вопросы на экзамен

	ный материал.	

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

Типовые вопросы к экзамену

Дисциплина:	Организационное и правовое обеспечение информационной безопасности	Специальность:	10.05.03.
Семестр:	V		
Кафедра:	Информационная безопасность		

1.	Правовое определение понятия «информация». Основные характеристики и свойства информации. Конфиденциальность информации. Обладатель конфиденциальной информации.
2.	Правовые последствия овеществления информации. Определение понятия «документированная информация».
3.	Правовое определение понятий: «информационные технологии», «информационные системы» и «информационно-телекоммуникационные сети». Объекты и субъекты информационных отношений.
4.	Защита информации. Правовое определение целей защиты информации.
5.	Основные права и обязанности органов ФСТЭК и ФСБ по защите информации.
6.	Понятие информационной безопасности. Основные виды угроз информационной безопасности России.
7.	Доктрина информационной безопасности об угрозах средствам информатизации, телекоммуникациям и средствам связи.
8.	Порядок лицензирования деятельности с использованием сведений, составляющих государственную тайну.
9.	Порядок лицензирования деятельности по технической защите конфиденциальных сведений.
10.	Сертификация средств защиты информации. Правовая ответственность за использование не сертифицированных средств защиты.
11.	Правовое значение лицензирования и сертификации в защите различных видов информации.
12.	Закон «О техническом регулировании». Технические регламенты и профили по защите информации.
13.	Государственные органы и органы исполнительной власти, отвечающие за защиту государственной тайны.
14.	Органы государственной власти и органы исполнительной власти, ответственные за защиту конфиденциальной информации.
15.	Основные разделы права и нормативно-правовые документы, регулирующие отношения в информационной сфере.
16.	Конституционные основы правовой защиты информации.
17.	Отражение вопросов защиты информации в законодательных и нормативных актах общего характера.
18.	Специальные законы, связанные с проблемами информатизации и защитой информации.
19.	Законодательство субъектов Российской Федерации, посвященное проблемам информатизации и защите информации.
20.	Уголовный кодекс Российской Федерации о защите информации.
21.	Гражданское право и защита информации. Нормы гражданского права, применимые для защиты информации.
22.	Кодекс Российской Федерации об административно-правовых нарушениях о защите информации.
23.	Общие правовые нормы и принципы, используемые для защиты информации.
24.	Роль и место закона «Об информации, информационных технологиях и защите информации» в структуре правовой защиты информации.
25.	Порядок защиты открытой, общедоступной информации. Правовая защита субъектов информационного

	процесса от «вредной информации».
26.	Роль и место закона «О персональных данных» в структуре правовой защиты информации.
27.	Понятие «Интеллектуальная собственность». Право авторства. Авторские права. Основные положения гражданского кодекса, защищающие авторские права.
28.	Порядок регулирования отношений между авторами, работодателями, изготовителями и распространителями объектов авторских прав. Лицензионные права.
29.	Основные положения гражданского кодекса, регулирующие отношения в сфере интеллектуальной собственности.
30.	Особенности правовой защиты интеллектуальной собственности. Контрафактная продукция. Правовая ответственность за распространение контрафактной продукции.
31.	Закон «Об электронной цифровой подписи», как средство правовой защиты информации в телекоммуникационных сетях.
32.	Информация с ограниченным доступом. Основные правовые документы, регламентирующие порядок защиты информации с ограниченным доступом.
33.	Информация, относительно которой запрещено вводить режим ограниченного доступа в соответствии с законом «Об информации, информационных технологиях и защите информации».
34.	Информация, относительно которой запрещено вводить режим коммерческой тайны.
35.	Принципы и порядок отнесения сведений к различным видам тайн.
36.	Порядок организации допуска и доступа к информации, составляющей различные виды тайн.
37.	Виды тайн, отнесённых к информации с ограниченным доступом.
38.	Административно-правовая и дисциплинарная ответственность за утечку информации с ограниченным доступом.
39.	Правовая ответственность за утечку информации, содержащей государственную тайну.
40.	Правовая защита служебной тайны.
41.	Правовая защита профессиональной тайны.
42.	Правовые аспекты защиты коммерческой тайны.
43.	Тайна следствия и судопроизводства.
44.	Персональные данные. Особый порядок правовой защиты персональных данных.
45.	Временные ограничения прав граждан, допущенных к государственной тайне и предоставляемые им социальные гарантии.
46.	Порядок засекречивания и рассекречивания сведений, содержащих государственную тайну.
47.	Роль ФСТЭК, ФСБ и Межведомственной комиссии в вопросах защиты государственной тайны.
48.	Особенности правовой защиты информации на предприятии. Основные нормативно-правовые и распорядительные документы, регулирующие отношения на предприятии по защите информации.
49.	Особенности правовой защиты информации в информационных и телекоммуникационных сетях, а также в сети Интернет. Ответственность за правонарушения и преступления, связанные с этими сетями.
50.	Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам.
51.	Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
52.	Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования.
53.	Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
54.	Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса.
55.	Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз.
56.	Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам.
57.	Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
58.	Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности.
59.	Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия».
60.	Структура и содержание документа «Политика информационной безопасности предприятия».
61.	Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия.
62.	Концепция информационной безопасности предприятия. Цели и задачи предприятия в обеспечении информационной безопасности при взаимодействии с внешними и внутренними субъектами информационного обмена.

63.	Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности предприятия». Принципы распределения полномочий.
64.	Процедуры и методы информационной безопасности предприятия как составляющие «Политики информационной безопасности предприятия». Профили защиты.
65.	Права и обязанности руководящего состава и сотрудников службы информационной безопасности. Роль служебных комиссий и «кризисных групп» в обеспечении информационной безопасности.
66.	Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию.
67.	Организация конфиденциального делопроизводства.
68.	Общие обязанности сотрудников по неразглашению конфиденциальной информации. Закрепление основных обязанностей в трудовом договоре.
69.	Организация доступа и допуска сотрудников к конфиденциальной информации.
70.	Порядок допуска предприятий к работам по созданию средств защиты конфиденциальной информации и к работам по оказанию услуг в области защиты конфиденциальной информации.
71.	Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа.
72.	Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией.
73.	Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности.
74.	Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией.
75.	Методы проверки кандидатов на работу. Отражение вопросов информационной безопасности в трудовых и коллективных договорах.
76.	Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания.
77.	Методы борьбы с нарушениями информационной безопасности. Порядок завершения текущей работы с сотрудниками, владеющими конфиденциальной информацией при их увольнении.
78.	Организация служебного расследования по фактам утечки конфиденциальной информации. Порядок проведения служебного расследования по фактам утраты секретных документов и разглашения конфиденциальной информации.
79.	Сложные инциденты. Порядок организации служебного расследования в случаях возникновения сложных инцидентов.
80.	Организация охраны объектов информатизации. Составные элементы системы охраны. Требования к охранникам и их обязанностям.
81.	Организация режима охраны объекта. Принципы охраны. Факторы, влияющие на выбор приёмов и средств охраны.
82.	Организация внутриобъектового и пропускного режимов на объектах информатизации. Цели организации внутриобъектового режима.
83.	Организация пропускного режима. Типы пропусков. Учёт пропускных документов.
84.	Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки.
85.	Порядок соблюдения объектового режима при работе с представителями сторонних организаций.
86.	Возможные каналы утечки информации из помещений, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. Требования СТР К по защите помещений. Организация борьбы с утечкой информации из помещений.
87.	Аттестация помещений, в которых обрабатывается конфиденциальная информация. Этапы проведения аттестации. Технический паспорт на помещение и аттестат соответствия.
88.	Порядок организации работ по созданию и эксплуатации объектов информатизации и средств защиты информации (СЗИ), определяемый СТР-К. Стадии создания объекты информации.
89.	Порядок организации эксплуатации автоматизированных систем и их средств защиты информации. Особенности защиты информации при использовании съемных накопителей информации большой емкости для АРМ на базе автономных ЭВМ.
90.	Порядок защиты информации в СУБД. Защита информации в локальных вычислительных сетях и при выходе в сети общего пользования.
91.	Организация защиты информации при взаимодействии со сторонниками организациями. Порядок отбора и подготовки информации к оглашению. Отражение вопросов защиты информации при подготовке договоров.
92.	Обеспечение защиты информации при ведении переговоров и при приеме в организации сторонних организаций и посетителей. Особенности обеспечения безопасности информации при приеме иностранных делегаций.
93.	Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвы-

	чайных ситуаций. Требования пожарной безопасности к объектам информатизации.

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

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебных занятий	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, самостоя-

	тельного 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. Контрольная работа должна полностью раскрывать содержание выбранной темы и оформляется в виде пояснительной записки (25-40 листов). Контрольная работа состоит из следующих разделов: 1 Введение 2 Аналитическая часть 3 Проектно – расчетная часть (в случае необходимости) 4 Заключение 5 Список литературных источников 6 Приложения (в случае необходимости) Контрольная работа обязательно должна иметь титульный лист, содержание, список сокращений, используемых в контрольной работе. Во *введении* обосновывается актуальный характер решения задачи, определяются цели домашнего задания и перечень основных проектных решений, формируемых в результате проводимых исследований, используемые методики, практическую значимость полученных результатов. В *аналитической части* проводится исследование задачи, сравнительный анализ средств и методов их решения, обосновывается выбор оптимального варианта проектных решений. Разрабатывается постановка задачи, определяются цели разработки системы защиты ИС, обосновывается ее необходимость и целесообразность, дается краткий анализ возможных методов решения поставленной задачи, а также анализируются ограничения и требования к программе. В *проектно – расчетной части* проводится разработка проектных решений по решению поставленной задачи. Приводится обоснование модели системы защиты ИС. Разрабатывается структура пользовательского интерфейса для реализации требований к создаваемому приложению, строится диалог пользователя в интерфейсе приложения. В *заключении* подводятся основные итоги контрольной работы и анализируются полученные результаты. *Список литературы* содержит перечень литературных источников и методических материалов, а также проектно – технической документации, используемой при подготовке домашнего задания. В *приложениях* приводятся распечатки, формы документов и другие дополнительные документы.
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: - в порядке, 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 научной проблемы. Количество и вес критериев оценки доклада зависят от того, является ли доклад единственным объектом оценивания или он представляет собой только его часть. 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 следующих критериев: - соответствие выступления теме, поставленным целям и задачам; - проблемность / актуальность; - новизна / оригинальность полученных результатов;

	- глубина / полнота рассмотрения темы; - доказательная база / аргументированность / убедительность / обоснованность выводов; - логичность / структурированность / целостность выступления; - речевая культура (стиль изложения, ясность, четкость, лаконичность, красота языка, учет аудитории, эмоциональный рисунок речи, доходчивость, пунктуальность, невербальное сопровождение, оживление речи афоризмами, примерами, цитатами и т.д.); - используются ссылки на информационные ресурсы (сайты, литература); - наглядность / презентабельность (если требуется); - 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 «Организационное и правовое обеспечение информационной безопасности»
(наименование дисциплины)

Правовое обеспечение информационной безопасности

Задание № 1.1

1. Дайте определение понятию «право».
2. Дайте определение понятию «правоотношение».
3. Назовите и охарактеризуйте необходимые элементы структуры правового отношения.
4. Чем определяется мера участия субъектов в правовых отношениях?
5. Назовите и охарактеризуйте составляющие состава правонарушения.
6. Назовите и охарактеризуйте виды юридической ответственности.
7. Что является предметом правового регулирования в информационной сфере?
8. Перечислите правовые принципы защиты информации.
9. Назовите и охарактеризуйте направления защиты информации.
10. Какие структуры власти участвуют в реализации государственной политики в сфере информатизации?
11. Назовите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации.
12. Перечислите основные задачи в области обеспечения национальной безопасности Российской Федерации.
13. Перечислите принципы технического регулирования.
14. Назовите задачи технического регулирования.
15. Назовите принципы обеспечения безопасности.

Задание № 1.2

16. Назовите функции системы безопасности Российской Федерации.
17. Перечислите основные задачи Совета безопасности Российской Федерации.
18. Перечислите основные виды тайн. Охарактеризуйте каждый вид.
19. Назовите обязательные признаки информации с ограниченным доступом.
20. На какие классы по функциональному назначению подразделяются документы по защите государственной тайны?
21. Дайте определение понятию «гриф секретности».
22. Какие сведения не относятся к государственной тайне и не подлежат засекречиванию?
23. Перечислите органы защиты государственной тайны.
24. Какие существуют методы защиты сведений, составляющих государственную тайну?

25. Опишите процедуру допуска должностных лиц и граждан к государственной тайне.
26. Какие сведения относятся к банковской тайне?
27. Перечислите известные вам виды профессиональной тайны.
28. Раскройте порядок обращения с документами, содержащими служебную тайну.
29. Какая информация относится к сведениям конфиденциального характера?
30. Какие сведения в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» запрещено относить к конфиденциальной информации?
31. Что представляет собой информация, составляющая коммерческую тайну?
32. Что понимается под разглашением информации, составляющей коммерческую тайну?
33. По каким признакам определяется перечень сведений, составляющих коммерческую тайну предприятия?
34. В отношении, каких сведений не может быть установлен режим коммерческой тайны?
35. Приведите меры по охране конфиденциальности информации в соответствии с законом «О коммерческой тайне».

Задание № 1.3

36. Назовите основные источники права в области защиты персональных данных.
37. Какие сведения являются предметом личной и семейной тайны?
38. Что понимается под обработкой персональных данных?
39. Перечислите принципы обработки персональных данных.
40. Какие требования необходимо выполнить при работе с персональными данными работника?
41. Перечислите основные законодательные акты, регламентирующие защиту интеллектуальной собственности.
42. Какие существуют институты защиты интеллектуальной собственности?
43. Перечислите и охарактеризуйте основные объекты интеллектуальной собственности.
44. Дайте определение понятиям «Изобретение», «полезная модель», «промышленный образец».
45. Назовите объекты патентного права.
46. Какие объекты патентного права не являются изобретениями?
47. Охарактеризуйте правовую основу защиты промышленного образца.
48. Перечислите и охарактеризуйте субъекты патентного права.
49. Перечислите объекты и субъекты авторского права.

Организационное обеспечение информационной безопасности

Задание № 2.1

1. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации.
2. Пути и проблемы практической реализации концепции комплексной защиты информации.
3. Криминалистическая характеристика компьютерного преступления. Основные способы совершения компьютерного преступления. Проблемы построение систем защищенного документооборота.
4. Виды реализации информационных угроз (перечислить, пояснить механизм реализации).
5. Виды реализации организационно-правовых угроз (перечислить, пояснить механизм реализации)
6. Виды реализации программных угроз (перечислить, пояснить механизмы реализации).
7. Виды реализации Internet угроз (перечислить, пояснить механизмы реализации)
8. Дать определение понятию «Политика безопасности».
9. Содержание документа Политика безопасности.

10. Содержание законодательных мер обеспечения информационной безопасности.
11. Содержание административных мер обеспечения информационной безопасности.
12. Содержание процедурных мер обеспечения информационной безопасности.
13. Цели и задачи организационной защиты информации, ее связь с правовой защитой информации.
14. Классификация технических каналов утечки информации. Каналы утечки информации в средствах и системах информатизации.
15. Виды угроз информационной безопасности на объекте защиты и их характеристика.

Задание № 2.2

16. Классификация технических каналов утечки информации. Каналы утечки информации из выделенных помещений.
17. Основные требования ФСТЭК к технической защите информации.
18. Средства и методы физической охраны объектов.
19. Основные способы осуществления мер обеспечения безопасности информации. Раскрыть содержание организационных (административных) мер.
20. Порядок проведения аттестации объектов информатизации. Этапы аттестации.
21. Модели нарушителей информационной безопасности на объекте.
22. Организационные мероприятия по защите конфиденциальной информации.
23. Основные организационно-распорядительные документы, разрабатываемые на объекте защиты.
24. Категории конфиденциальности информации. Что относится к информации первой категории.
25. Структура органов по защите информации в РФ.
26. Функции и задачи службы безопасности объекта информатизации.
27. Требования защищенности СВТ от НСД к информации. Классы и группы защищенности СВТ от НСД.
28. Типовая структура службы безопасности. Задачи, решаемые подразделениями службы безопасности.

Задание № 2.3

29. Исходные данные по аттестуемому объекту информатизации.
30. Основные документы, регламентирующие деятельность подразделения (специалиста) по защите информации.
31. Требования к помещениям, в которых циркулирует защищаемая информация. Категорирование помещений. Определение границ контролируемых зон (КЗ).
32. Организация обучения персонала, ее методы и формы.
33. Требования руководящих документов по порядку разработки и содержанию «Положения о подразделении (специалисте) по защите информации».
34. Организационные мероприятия, проводимые с целью защиты СВТ и АС от НСД.
35. Требования руководящих документов по порядку разработки и содержанию «Руководства по защите информации …».
36. Типовой перечень внутренних организационно-распорядительных документов по защите конфиденциальной информации.
37. Основные направления обеспечения защиты информации от НСД.
38. Положение по аттестации объектов информатизации.
39. Основные принципы защиты информации от НСД.
40. Порядок согласования и утверждения Руководства по защите информации.
41. Оценка класса защищенности средств вычислительной техники (сертификация СВТ).
42. Объекты обеспечения информационной безопасности РФ во внутренней политике?
43. Угрозы информационной безопасности РФ в сфере внутренней политики?

Критерии оценки

«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

по дисциплине «Организационное и правовое обеспечение информационной безопасности»

(наименование дисциплины)

Задание №1

1. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
2. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
3. Правовые основы защиты конфиденциальной информации.
4. Организационные основы защиты конфиденциальной информации.
5. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
6. Построение и функционирование защищенного документооборота.
7. Анализ инструкции по обработке и хранению конфиденциальных документов.
8. Направления и методы защиты документов на бумажных носителях.
9. Направления и методы защиты машиночитаемых документов.
10. Направления и методы защиты электронных документов.

Задание № 2

11. Направления и методы защиты аудио и визуальных документов.
12. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
13. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
14. Соотношение источников, каналов распространения и каналов утечки информации.
15. Анализ опыта защиты информации в зарубежных странах.
16. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
17. Основы технологии обработки и хранения конфиденциальных документов.
18. Назначение, виды, структура и технология функционирования системы защиты информации.

Задание № 3

19. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
20. Направления и методы защиты профессиональной тайны.
21. Направления и методы защиты служебной тайны.
22. Направления и методы защиты персональных данных о гражданах.
23. Защита секретов в дореволюционной России.
24. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.
25. Порядок подбора персонала для работы с конфиденциальной информацией.
26. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.
27. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
28. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.
29. Задачи, функции и графическая структура служб конфиденциальной документации в фирмах различных типов, нормативно-методическое обеспечение их деятельности.
30. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

Задание № 4

31. Аналитический обзор различных технологий хранения конфиденциальных документов.
32. Назначение, виды и технология учета конфиденциальных документов.
33. Составление библиографии по проблемам экономической безопасности, защиты предпринимательской тайны и конфиденциальной информации (российская и зарубежная литература).
34. Процессуальные проблемы защиты информации в зарубежных странах.
35. Анализ существующих схем доступа персонала в помещения фирмы.
36. Аналитический обзор опыта зарубежных стран в регламентации управления персоналом, обладающим конфиденциальной информацией.
37. Аналитический обзор российского и зарубежного исторического опыта в предотвращении утраты ценной информации по вине сотрудников.
38. Анализ существующих правил поведения персонала и охраны фирмы в экстремальных ситуациях различного типа.
39. Проблемы управления персоналом и защиты информации в предпринимательской деятельности (теоретический очерк).

Задание № 5

40. Психологические и профессиональные особенности личности человека, владеющего тайной, мотивации мышления и поведения.
41. Цели, задачи, стадии и методы работы с персоналом, обладающим конфиденциальной информацией.
42. Технологическая схема приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией.
43. Классификация персонала фирмы и окружающих фирму людей по степени их осведомленности в тайнах фирмы, анализ каждой классификационной группы.
44. Классификация экстремальных ситуаций, угрожающих персоналу фирмы в рабочее и нерабочее время, анализ выделенных классификационных групп и методов локализации опасности.
45. Порядок и методика проведения служебного расследования по фактам нарушения правил защиты секретов фирмы.
46. Факторы, предпосылки и условия применения различных форм морального и материального стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы.
47. Место и роль психологического климата в коллективе при проведении воспитательной работы в коллективе фирмы.
48. Классификация противоправных действий персонала фирмы с конфиденциальной информацией.
49. 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 задания

Дисциплина:	Организационно-правовое обеспечение информационной безопасности	Специальность:	10.05.03.
Семестр:	V		
Кафедра:	Информационная безопасность		

Задание А

1.	Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи? а) Правовые. б) Организационно-технические. в) Экономические. г) Стратегические.
2.	Какую задачу решает сертификация средств защиты информации? а) Обеспечения требуемого качества защиты информации. б) Повышения квалификации разработчиков средств защиты информации. в) Создания надежных средств защиты информации. г) Защиты отечественных производителей средств защиты информации.
3.	На решение каких вопросов направлена система лицензирования деятельности в области защиты государственной тайны? а) На выполнение требований к организациям и лицам, занимающимся вопросами защиты государственной тайны. б) На повышение экономической эффективности деятельности в области защиты государственной тайны. в) На обеспечение правовых основ деятельности в области защиты государственной тайны. г) На решение проблемы надлежащего финансирования работ в области защиты государственной тайны.
4.	Частью какой, более общей системы, является система обеспечения информационной безопасности Российской Федерации? а) Системы защиты национальных интересов страны. б) Системы обороны страны. в) Системы защиты прав граждан страны. г) Системы обеспечения национальной безопасности страны.
5.	Какие действия квалифицируются как компьютерное пиратство? а) Незаконное тиражирование лазерных дисков. б) Распространение незаконно полученной информации по компьютерным сетям. в) Попытка получить санкционированный доступ к компьютерной системе или вычислительной сети. г) Попытка получить несанкционированный доступ к компьютерной системе или вычислительной сети.
6.	Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется: а) Достоверной. б) Конфиденциальной. в) Документированной. г) Коммерческой тайной.

7.	Какой из следующих законов еще не принят? а) «О правовой информации». б) «О праве на информацию». в) «О персональных данных». г) «О защите детей от информации, причиняющей вред их здоровью и развитию».
8.	Какая информация не относится к государственной тайне (в соответствии с законом «О государственной тайне» и указом Президента №1203)? а) Информация о военной отрасли. б) Информация о внешнеполитической деятельности. в) Информация о методах и средствах защиты секретной информации. г) Информация о размерах золотого запаса страны.
9.	К органам, уполномоченным на ведение лицензированной деятельности на право проведения работ, связанных с созданием средств защиты информации относятся: а) ФАПСИ. б) ФСТЭК. в) ФСБ и СВР. г) Организации, указанные в п.1 и п.2.
10.	Система правовых норм, которыми определяется порядок охраны изобретений, полезных моделей, промышленных образцов и селекционных достижений путем выдачи патентов – это: а) Авторское право. б) Патентное право. в) Право на секреты производства. г) Интеллектуальное право.
11.	Выберите верное утверждение: а) Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. б) Право искать, получать, передавать производить и распространять информацию может быть ограничено в случае введения чрезвычайного положения. в) Конституция гарантирует охрану интеллектуальной собственности. г) Юридическая сила электронной подписи определяется законом «О правовой охране программ для ЭВМ и баз данных».
12.	Выберите верное утверждение: а) Наказание за неправомерный доступ к охраняемой законом компьютерной информации установлено Гражданским Кодексом РФ. б) База данных является объектом интеллектуальной собственности. в) Программы могут выступать в качестве нематериальных активов предприятия. г) Автором программ является юридическое или физическое лицо, на средство которого создана программа.
13.	Конституция РФ принята: а) в 1991г. б) в 1995г. в) в 1993г. г) в 2002г.
14.	Право свободно получать, производить и распространять информацию закреплено: а) в Конституции РФ. б) в законе «Об информации, информатизации и защите информации». в) в Гражданском Кодексе. г) в Уголовном Кодексе.
15.	Понятие служебной и коммерческой тайны сформулировано: а) в Конституции РФ. б) в ФЗ «Об информации, информатизации и защите информации». в) в Гражданском Кодексе. г) в Уголовном Кодексе.

16.	Права собственника информационных ресурсов определены: а) в Конституции РФ. б) в законе «Об информации, информатизации и защите информации». в) в Гражданском Кодексе. г) в Уголовном Кодексе.
17.	Наказание за распространение компьютерных вирусов установлено: а) в Конституции РФ. б) в законе «Об информации, информатизации и защите информации». в) в Гражданском Кодексе. г) в Уголовном Кодексе.
18.	Юридическая основа использования электронной подписи закреплена: а) в законе «Об информации, информатизации и защите информации». б) в законе «Об авторском праве и смежных правах. в) в законе «О правовой охране программ для ЭВМ и баз данных». г) в Гражданском Кодексе.
19.	Права автора программ определены: а) в законе «Об информации, информатизации и защите информации». б) в законе «Об авторском праве и смежных правах. в) в законе «О правовой охране программ для ЭВМ и баз данных». г) в Гражданском Кодексе.
20.	Перечень видов информации, доступ к которым не может быть ограничен, определен: а) в законе «Об информации, информатизации и защите информации». б) в законе «Об авторском праве и смежных правах. в) в законе «О правовой охране программ для ЭВМ и баз данных». г) в Гражданском Кодексе.
21.	Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан? а) Указ Президента РФ. б) Закон «Об информации, информатизации и защите информации». в) Закон «О правовой охране программ для ЭВМ и баз данных. г) Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ.
22.	Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере? а) Неправомерный доступ к компьютерной информации. б) Создание, использование и распространение вредоносных программ для ЭВМ. в) Умышленное нарушение правил эксплуатации ЭВМ и их сетей. г) Все перечисленное выше.
23.	Можно ли использовать статьи из разных журналов и газет на политические, экономические, религиозные или социальные темы для подготовки в качестве учебного материала? а) Нет. б) Да, указав источники заимствования. в) Да, указав ФИО авторов и название статей. г) Да, не спрашивая согласия правообладателей, но с обязательным указанием источника заимствования и имен авторов.
24.	Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения? а) Уголовный кодекс РФ. б) Гражданский кодекс РФ. в) Доктрина информационной безопасности РФ. г) Постановления Правительства РФ.

25.	За нарушения законодательства РФ о ГТ предусматривается (...) ответственность: а) Уголовная и административная б) Гражданско-правовая в) Дисциплинарная г) Указанная в п.1-3
26.	Срок засекречивания сведений, составляющих государственную тайну: а) Составляет 10 лет. б) Ограничен 30 годами. в) Устанавливается Указом Президента РФ. г) Ничем не ограничен.
27.	Предельный срок пересмотра ранее установленных грифов секретности составляет: а) 5 лет. б) 1 год. в) 10 лет. г) 15 лет.
28.	Документы, содержащие государственную тайну снабжаются грифом: а) "Секретно". б) "Совершенно секретно". в) "Особой важности". г) Указанным в п.1-3.
29.	«Ноу-хау» это - а) Незащищенные новшества. б) Защищенные новшества. в) Общеизвестные новые технологии. г) Опубликованные технические и технологические новинки.
30.	Формой правовой защиты литературных, художественных и научных произведений является (...) право: а) Литературное. б) Художественное. в) Авторское. г) Патентное.

Вопросы рассмотрены и утверждены на заседании кафедры	Дата: _____ г.	Протокол № ___
Заведующий кафедрой	подпись	ФИО

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

Типовые контрольные работы

Дисциплина:	Организационно-правовое обеспечение информационной безопасности	Специальность:	10.05.03.
Семестр:	V		
Кафедра:	Информационная безопасность		

ЗАДАНИЕ Б

1. История и современные направления защиты информации.
2. Правовая основа защиты информации за рубежом.
3. Правовая основа защиты информации в России.
4. Засекречивание информации. Политический и социальный аспекты засекречивания информации.
5. Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.
6. Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.
7. Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.
8. Защита информации, составляющей профессиональную тайну.
9. Защита информации, составляющей банковскую тайну.
10. Защита сведений, составляющих личную тайну.
11. Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.
12. Система защиты информации, ее структурная и функциональная части.
13. Уголовная ответственность за государственную измену, шпионаж, разглашение государственной тайны и утрату секретных документов, объективная и субъективная сторона этих преступлений.
14. Политика безопасности предприятий.
15. Принципы информационной безопасности предприятия.
16. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности.
17. Структура организации защиты информации предприятия.
18. Система защиты информации предприятия.
19. Лицензирование в области защиты конфиденциальной информации.
20. Разработка регламента организации и проведения специальных экспертиз предприятий.
21. Оформления запроса на лицензирование деятельности в области защиты информации.
22. Разработка методики допуска к сведениям, составляющим государственную тайну.
23. Разработка комплекта документов при оформлении допуска к государственной тайне.
24. Разработка методики доступа к сведениям составляющим государственную тайну, при командировании в другие организации.
25. Разработка комплекта документов по обеспечению сохранности документов, дел и изданий.
26. Разработка обязанностей лиц, допущенных к сведениям, составляющих коммерческую тайну.
27. Инструкция по организации контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
28. Обязанности персонала организации по сохранению коммерческой тайны.

29. Состав и структура системы безопасности предприятия.
30. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
31. Направления работы по обучению персонала, допускаемого к конфиденциальной информации.
32. Организация информационно – аналитической работы на предприятии.
33. Организация охраны предприятий.
34. Основные задачи организации режима и охраны.
35. Организация пропускного режима на предприятии.
36. Разработка комплекта документов при организации пропускного режима на предприятии.
37. Разработка комплекта документов, реализующих требования внутриобъектового режима.
38. Основные документы, разрабатываемые на охраняемых объектах.
39. Разработка комплекта документов при проведения аттестационных испытаний защищаемых объектов.

Критерии оценивания выполнения тестирования

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 выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала в области 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 от 50% до 59%.

2 «Неудовлетворительно» - процент правильно выполненных заданий составляет менее 50%.

Критерии оценивания выполнения контрольных работ

Контрольная работа, выполненная студентом, может быть либо зачтена, либо не зачтена. Каждый преподаватель индивидуально и объективно оценивает работу по пяти бальной шкале, руководствуясь при этом следующими критериями.

Оценка **«отлично»** выставляется за контрольную работу, в которой:

1. Представлено логичное содержание.
2. Отражена актуальность рассматриваемой темы, верно определены основные категории.
3. Дан анализ литературы по теме, выявлены методологические основы изучаемой проблемы, освещены вопросы истории ее изучения в науке. Анализ литературы отличается глубиной, самостоятельностью, умением показать собственную позицию по отношению к изучаемому вопросу.
4. В заключении сформулированы развернутые, самостоятельные выводы по работе.
5. Работа оформлена в соответствии с разработанными в колледже требованиями, написана с соблюдением норм литературного языка.

6. Работа выполнена в срок.

Оценка **«хорошо»** выставляется за контрольную работу, в которой:

1. Представлено логичное содержание.
2. Раскрыта актуальность темы, верно определены цель и задачи.
3. Представлен круг основной литературы по теме, выделены основные понятия, используемые в работе. Обобщен педагогический опыт, выявлены его сильные и слабые стороны. В отдельных случаях студент не может дать критической оценки взглядов исследователей, недостаточно аргументирует отдельные положения.
4. В заключении сформулированы общие выводы.
5. Работа оформлена в соответствии с разработанными в колледже требованиями, написана с соблюдением норм литературного языка. В ней отсутствуют орфографические и пунктуационные ошибки. Допустимы отдельные погрешности стиля.
6. Работа выполнена в срок.

Оценкой **«удовлетворительно»** оценивается контрольная работа, в которой;

1. Представлено логичное содержание.
2. Актуальность темы раскрыта правильно, но список литературы ограничен.
3. Теоретический анализ дан описательно, студент не сумел отразить собственной позиции по отношению к рассматриваемым материалам, ряд суждений отличается поверхностностью.
4. В заключении сформулированы общие выводы.
5. Работа оформлена в соответствии с разработанными в колледже требованиями, в ней имеются орфографические и пунктуационные ошибки, погрешности стиля.
6. Работа выполнена в срок.

Оценкой **«неудовлетворительно»** оценивается контрольная работа, в которой большая часть требований, предъявляемых к работам, ***не выполнена***.

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 краткими пояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:

- умения применять математические методы для формализации и решения прикладных задач; строить модели экономических процессов, исследовать их и вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения экономических объектов, систем, процессов;
- владение навыками работы с пакетами прикладных программ для моделирования и анализа экономических процессов.

в) описание шкалы оценивания

- **«Зачтено»** выставляется в случае, если студент выполнил в полном объеме лабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагает этапы решения и результаты работы.

- **«Незачтено»** выставляется в случае, если студент не выполнил лабораторную работу, либо выполнил, но допустил существенные ошибки в расчетах и (или) не сделал выводы, и (или) не может изложить этапы решения и результаты работы.

Критерии оценивания экзамена

Критерии оценок на **экзамене** 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.

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

Фонд оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 1 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к экзамену, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к экзамену, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к экзамену	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к экзамену, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;
– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

БГАРФ	Балтийская государственная академия рыбопромыслового флота		
	Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»		
	Версия: 1	Дата выпуска версии: 27.02.17	стр. 38 из 38

Формат сведений о ФОС и ее согласовании

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

Б1.Б.29 «Организационное и правовое обеспечение информационной безопасности»
(код) (наименование дисциплины)

образовательной программы специалитета по специальности
10.05.03. Информационная безопасность автоматизированных систем

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

утвержденной «27» июня 2018 г.

Автор фонда – доцент кафедры ИБ Жестовский А.Г.

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

(протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой _____/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 _____/А.Г. Жестовский/

Согласовано

Начальник отдела мониторинга и контроля

_____/Борисевич Ю.В./