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)

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(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.32 «Управление информационной безопасностью»
(код) (наименование дисциплины)

№ п/п	Контролируемые модули, разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Оценочные средства	Способ контроля
			наименование	
1	Тема 1. Введение.	ОК-4, ОПК-6	собеседование, контрольная работа	устный письменный
2	Тема 2. Система управления информационной безопасностью автоматизированных систем.	ОК-4, ОПК-6, ПК-4, ПК-6, ПК-13, ПК-25	собеседование, контрольная работа, защита практического занятия	устный письменный
3	Тема 3. Политика безопасности автоматизированных систем.	ОК-4, ОПК-6, ПК-4, ПК-11, ПК-22, ПК-24, ПСК-7.2	коллоквиум, доклад, защита практического занятия	устный письменный
4	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем.	ОПК-6, ПК-6, ПК-22, ПК-28	защита практического занятия	устный
5	Тема 5. Аудит информационной безопасности автоматизированных систем.	ОПК-6, ПК-3, ПК-6, ПК-24, ПК-25, ПК-26, ПК-28, ПСК-7.2	собеседование, контрольная работа, защита практического занятия	устный письменный
6	Тема 6. Средства поддержки процессов управления информационной безопасностью АС.	ОПК-6, ПК-3, ПК-6, ПК-24, ПК-25, ПК-26, ПК-28, ПСК-7.2	собеседование, контрольная работа, защита практического занятия	устный письменный

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.32 «Управление информационной безопасностью»

(код) (наименование дисциплины)

№ п/п	Код компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студенты должны:		
			знать	уметь	владеть
1.	ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права; правовые основы обеспечения национальной безопасности Российской Федерации	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
2.	ОПК-6	способность применять нормативные правовые акты в профессиональной деятельности	основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информа-	применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; разрабатывать и исследовать аналитические и ком-	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; навыками использования программно-аппаратных средств обеспечения инфор-

			ции; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России	пьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; администрировать подсистемы информационной безопасности автоматизированных систем; пользоваться нормативными документами по противодействию технической разведке; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	мационной безопасности автоматизированных систем
3.	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 организации и обеспечения режима секретности

4.	ПК-4	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; анализировать и оценивать угрозы информационной безопасности объекта	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации
5.	ПК-6	способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования ПО	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
6.	ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать частные политики информационной	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

				безопасности информационной безопасности автоматизированных систем	
7.	ПК-13	способность участвовать в проектировании средств защиты информации автоматизированной системы	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности автоматизированных систем	методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации
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 автоматизированных систем	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем

9.	ПК-24	способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; основные методы управления информационной безопасностью	восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; разрабатывать частные политики информационной безопасности автоматизированных систем	навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками организации и обеспечения режима секретности; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
10.	ПК-25	способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации	использовать средства ОС для обеспечения эффективного и безопасного функционирования АС; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; проводить выбор программно-аппаратных средств обеспечения ИБ для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности АС	навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; методами формирования требований по защите информации; навыками, эксплуатации и администрирования баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками

11.	ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах	планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; администрировать подсистемы информационной безопасности автоматизированных систем	навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; 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
12.	ПК-28	способность участвовать в управлении информационной безопасностью автоматизированной системы	основные методы управления информационной безопасностью	разрабатывать предложения по совершенствованию системы управления информационной безопасностью АС	методами управления информационной безопасностью автоматизированных систем
13.	ПСК-7.2	способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных систем	принципы проведения аудит защищенности информационно-технологических ресурсов распределенных информационных систем	проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем; использовать методики аудита защищенности информационно-технологических ресурсов распределенных ИС	методиками проводить аудит защищенности информационно-технологических ресурсов распределенных ИС, с использованием средств проведения аудита

ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.32 «Управление информационной безопасностью»
(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.	ОК-4	+	+	+	+								
2.	ОПК-6	+	+	+	+	+	+	+	+	+	+	+	+
3.	ПК-3								+	+	+	+	+
4.	ПК-4				+	+	+						
5.	ПК-6		+	+				+	+	+	+	+	+
6.	ПК-11					+	+						
7.	ПК-13			+	+								
8.	ПК-22						+	+	+				
9.	ПК-24						+	+	+		+	+	+
10.	ПК-25		+	+						+	+	+	+
11.	ПК-26										+	+	+
12.	ПК-28									+	+	+	+
13.	ПСК-7.2					+	+			+	+	+	+

ПОКАЗАТЕЛИ И КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ п/п	Код контролируемой компетенции (или ее части)	Уровни сформированности компетенции		
		пороговый	продвинутый	высокий
1	ОК-4	Знать:		
		профессиональную терминологию	законодательные акты, нормативно-методические документы, определяющие особенности функционирования предприятий и организаций в информационной сфере	основные подходы к оценке правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности комплекса мер по информационной безопасности
		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	осуществлять выбор мероприятий по обеспечению информационной безопасности объектов и систем профессиональной деятельности на основе многокритериальной оценки, включающей правовые аспекты
		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
2	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 законодательства, в том числе с помощью систем правовой информации	применять действующую законодательную базу в области информационной безопасности	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационных документов, анализировать эффективность систем организаци-

				онной 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
3	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
4	ПК-4	Знать:		
		основные этапы проведения анализа уязвимости объекта, при разработке модели угрозы и модели нарушителя	основные виды моделей воздействия нарушителей информационной безопасности АС	основные модели и методики оценки показателей уязвимости (устойчивости), реализуемые при создании эффективной системы безопасности
		Уметь:		
		классифицировать возможные виды ущерба от нарушения безопасности информации в АС	оценивать влияние угроз информационной безопасности АС на тактико-технические характеристики аппаратных средств обработки информации	производить оценку снижения эффективности процесса обработки информации, вызванного ухудшением ТХ аппаратных средств, качества программных средств, исходной и обрабатываемой информации в 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

5	ПК-6	Знать:		
		порядок разработки, внедрения и эксплуатации автоматизированных систем, отвечающих требованиям информационной безопасности	организацию обеспечения информационной безопасности при эксплуатации защищенных АС	основные средства анализа защищенности 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
6	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
7	ПК-13	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 си-	навыками работы с нормативно-правовыми актами	методологией прикладных научных исследований в предметной области

		стемы организационной защиты информации		
8	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 вопросам защиты информации	разрабатывать функциональные обязанности должностных лиц организации по вопросам защиты информации	разрабатывать функциональные обязанности должностных лиц организации 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
9	ПК-24	Знать:		
		основные способы оптимизации процедуры оценки соответствия требованиям защищенности автоматизированных систем	порядок создания систем информационных технологий, удовлетворяющих требованиям информационной безопасности	порядок разработки профиля защиты и задания по информационной безопасности, защищенных АС
		Уметь:		
		исследовать эффективность создаваемых защищенных средств автоматизации	проводить технико-экономическое обоснование применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	реализовывать планы обеспечения бесперебойной работы организации для случаев вирусного заражения и планы резервного копирования всех необходимых данных и программ и их восстановления
		Владеть:		
		навыками разработки нормативных материалов по регламентации системы защиты информации	навыками работы с нормативно-правовыми актами	методологией прикладных научных исследований в предметной области
10	ПК-25	Знать:		
		организационные основы эксплуатации защищенных АС	порядок обеспечения бесперебойной работы систем защиты информации в АС при возникновении нештатных ситуаций	основной порядок предотвращения и восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций
		Уметь:		
		планировать подготовку персонала организации (предприятия) при возникновении нештатных ситуаций	принимать соответствующие меры по обнаружению внедрения вредоносного программного обеспечения АС и ликвидации последствий его атак	реализовывать планы обеспечения бесперебойной работы организации для случаев вирусного заражения и планы резервного копирования всех необходимых данных и программ

		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
11	ПК-26	Знать:		
		принципы работы средств обеспечения безопасности	принципы построения и функционирования сетей и протоколов стека TCP/IP	работу сетей. IP адресация, модели ISO OSI, TCP
		Уметь:		
		производить поиск уязвимостей с помощью специализированного ПО и их устранение	настраивать систему защиты от НСД на базе Windows	настраивать антивирусные системы
		Владеть:		
		навыками поддержки работоспособности, администрирования и обеспечения бесперебойной работы специальных средств защиты информации	навыками проведения аудитов, подготовки организационно-распорядительной документации и отчетов по ИБ	навыками мониторинга и контроля функционирования средств обеспечения ИБ
12	ПК-28	Знать:		
		нормативные и методические материалы по обеспечению защиты информации и соблюдению государственной тайны и конфиденциальной информации	методы и процедуры выявления угроз безопасности информации на объектах информатизации организации	порядок, методы и средства выявления угроз безопасности информации в ключевых системах информационной инфраструктуры
		Уметь:		
		участвовать в разработке новых средств автоматизации контроля, схем аппаратуры контроля, моделей и систем защиты информации	устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации	разрабатывать предложения по совершенствованию и повышению эффективности средств информационной безопасности
		Владеть:		
		навыками администрирования различных операционных систем, настройки и поддержки антивирусного ПО	навыками администрирования различных операционных систем, настройки и поддержки антивирусного ПО	навыками проведения сравнительного анализа характеристик (показателей) разных классов средств обеспечению безопасности информации
13	ПСК-7.2	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; - 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 систематизировать важнейшие материалы изучаемого курса, развить способность логично и содержательно выражать свои мысли в письменной форме. Необходимость создания рабо-	Образец рабочей тетради

	чей 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.	
Индивидуальное задание (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 заданий
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 (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

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, 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. 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.
Индивидуальное задание (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 прописы-

	ваются 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 афоризма-

	ми, 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

ТИПОВЫЕ ВОПРОСЫ К ЗАЧЕТУ*

Дисциплина:	Управление информационной безопасностью	Специальность:	10.05.03.
Семестр:	А		
Кафедра:	Информационная безопасность		

1.	Основные понятия информационной безопасности. Защита информации. Управление информационной безопасностью. Модель безопасности. Прямое воздействие.
2.	Понятие защищенной системы.
3.	Как изменялся подход к задаче защите информации? Три этапа развития защиты информации.
4.	Теория защиты информации. Основные составные части теории защиты информации.
5.	Современная постановка задачи защиты информации.
6.	Угроза, атака, источники угроз. Что такое окно опасности. Критерии классификации угроз.

7.	Наиболее распространенные угрозы доступности.
8.	Программные угрозы доступности.
9.	Основные угрозы целостности. Статическая и динамическая целостность.
10.	Основные угрозы конфиденциальности.
11.	Таксономия угроз безопасности. Что такое уязвимость защиты? Таксономия угроз безопасности. Ошибки в системах защиты.
12.	Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ.
13.	Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа.
14.	Понятие политики и модели безопасности. Структура монитора обращений.
15.	Методы идентификации и аутентификации. Способы аутентификации – пользователь «знает», пользователь «имеет» и пользователь «есть».
16.	Базовые представления моделей безопасности. Субъекты, объекты и доступ.
17.	Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Модель Харрисона-Руззо-Ульмана..
18.	Мандатная модель Белла-Лападулы. Свойство простой безопасности. Свойства ограничения. Свойство самостоятельной защиты. Правила перехода.
19.	Какая главная задача стандартов информационной безопасности? «Оранжевая книга» США. Базовые требования безопасности. Четыре группы критериев безопасности.
20.	Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.
21.	Основные руководящие документы Гостехкомиссии по вопросам защиты от несанкционированного доступа к информации. Классы защищенности.
22.	ГОСТ Р ИСО МЭК 15048-2002 «Общие критерии оценки безопасности информационных технологий». Профиль защиты. функции безопасности. Предложения безопасности.
23.	Основные функции организационно-правовой базы защиты информации. Виды информационных ресурсов. Какую информацию относят к защищаемой?
24.	Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».
25.	Криптографические механизмы и примитивы. Базовые методы преобразования информации используемые в криптографии. Основные группы методов защитных преобразований. Методы перестановки, подстановки, аддитивные и комбинированные.
26.	Криптография с симметричными ключами. Алгоритм DES, ГОСТ 28147-80., IDEA. Преимущества и недостатки криптографии с симметричными ключами.
27.	Ассиметричные алгоритмы шифрования. Криптосистема с открытым ключом RSA. ХЭШ-функция. Понятие односторонней функции. Коллизия хэш-функции.
28.	Иерархический метод разработки защищенных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB).

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

ВОПРОСЫ ДЛЯ КОЛЛОКВИУМОВ, СОБЕСЕДОВАНИЯ

по дисциплине

«Управление информационной безопасностью»

(наименование дисциплины)

1. Из каких элементов состоит трёхуровневая модель оценки защищенности информационной системы?
2. Какими путями осуществляется стандартизация подходов к обеспечению информационной безопасности и какие международные стандарты для этого применяются?
3. Какие уровни реализуются в технологической модели подсистемы информационной безопасности ИС?
4. С какой целью производится шифрование данных и информации и на каком уровне работы с информацией это применяется?
5. Что такое «единое информационное пространство»? Каковы его составляющие?
6. В каком случае возникает несовместимость вычислительных, информационных и телекоммуникационных устройств?
7. Как можно определить понятие «открытая информационная или программная система»?
8. Какими свойствами обладает открытая система?
9. Что такое итология и какие методы лежат в основе итологии?
10. Какие организации образуют структуру международной стандартизации в области информационных технологий?
11. Какие международные организации занимаются вопросами стандартизации в среде Web-сервисов?
12. Что составляет методологическую основу базиса открытых систем?
13. Какие прикладные программы работают в функциональной среде открытых систем?
14. В чём состоит суть эталонной модели взаимосвязи открытых систем (Open Systems Interconnection)?
15. Сколько уровней взаимодействия содержит модель ВОС? Какие это уровни?
16. Каким образом определяют понятие «профиль открытой системы»?
17. Что является базовой основой профиля?
18. С какой целью была разработана таксономия профилей?
19. Что включает в себя международный стандартизированный профиль ISP?
20. Для чего разработан профиль переносимости приложений APP и какое отношение он имеет к профилю GOSIP?
21. Какие четыре основных типа интерфейсов OSE вводит классификация интерфейсов открытых систем?
22. Что является основными целями разработки OSE и OSI профилей?
23. Каким образом и с помощью каких профилей связаны архитектурный и функциональный уровни открытой информационной системы?
24. Что включает в себя процесс проектирования профиля открытой системы?
25. Какие основные функциональные профили выбираются, компонуются и применяются на стадиях реализации жизненного цикла информационной системы?
26. Какие два основных значения имеет термин Internet?
27. Какие информационные услуги реализуют Internet-службы?
28. Что такое пространство Intranet и чем оно отличается от пространства Internet?
29. Перечислите основные архитектуры компьютерных сетей.
30. Приведите классификацию компьютерных сетей по различным классификационным признакам.

31. Какие топологии локальных компьютерных сетей существуют? Определите преимущества и недостатки каждой топологии.
32. Назовите основные физические архитектуры локальных компьютерных сетей.
33. Что является содержанием понятия «экономическая безопасность предприятия?
34. Как можно охарактеризовать понятие «информационная безопасность» и что оно в себя включает (основные составляющие)?
35. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?
36. Для чего необходимо формировать политику информационной безопасности и из каких основных разделов она состоит?
37. Кто разрабатывает политику информационной безопасности предприятия? Какие менеджеры и специалисты входят в рабочую группу?
38. Какие вопросы информационной безопасности являются ключевыми?
39. Из чего складывается инфраструктура информационной безопасности?
40. Какие существуют виды угроз ИБ и каким образом оцениваются соответствующие риски?
41. На какие виды подразделяется защищаемая информация?
42. Что включает в себя модель информационной безопасности?
43. В каких аспектах рассматриваются мероприятия по защите информации?
44. Каким образом оценивается соотношение эффективности и рентабельности систем информационной безопасности?
45. В каком случае информационная система считается защищенной?
46. Каким образом архитектура информационной системы может способствовать общей информационной безопасности и почему?
47. Чем отличается схема симметричной криптосистемы с закрытым ключом от схемы асимметричной криптосистемы с открытым ключом?
48. Что такое VPN и для каких целей используются эти технологии?
49. Какие типы вирусов выделены в настоящее время?
50. Какие существуют общие правила для пользователей для обеспечения антивирусной безопасности?
51. Каким общим требованиям должен удовлетворять качественный антивирусный программный продукт?

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ

Дисциплина:	Управление информационной безопасностью	Специальность:	10.05.03.
Семестр:	A		
Кафедра:	Информационная безопасность		

1.	Что такое домен безопасности? a) собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров b) виртуальная частная сеть с единым центром управления c) локальная сеть, не имеющая выхода в сети связи общего пользования d) сетевая операционная система
2.	Какое из требований необязательно для операционных систем, сертифицированных по 5 классу РД СВТ? a) Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ b) ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа c) Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов) d) В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа
3.	Присутствуют ли в ОС семейства Windows механизмы, осуществляющие криптографические преобразования? a) нет b) присутствуют механизмы ЭЦП и хеширования c) присутствуют механизмы обмена ключами d) присутствуют механизмы для симметричного шифрования данных
4.	Что такое PAM? a) набор библиотек подключаемых модулей шифрования b) набор открытых библиотек подключаемых модулей аутентификации c) набор открытых библиотек подключаемых модулей резервного восстановления d) набор открытых библиотек подключаемых модулей доверенной загрузки
5.	1. Открытой распределенной информационной системой (open distributed information system) называется система: a. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики b. располагающая службами, пользование которыми возможно при использовании специальных синтаксиса и семантики c. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики d. не располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

6.	Угроза это: a) совокупность сообщений, направленных на запугивание b) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу. c) совокупность сообщений, направленных на причинение вреда d) любое действие, направленное на причинение ущерба
7.	Классами защищённости автоматизированных систем от несанкционированного доступа являются: a) 1Е b) 2А c) 2В d) 3Б
8.	Определите класс автоматизированной системы по следующим классификационным признакам: *АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается “Комерческая тайна”.* a) 2Б b) 1Г c) 1Д d) 3Б
9.	Определите класс автоматизированной системы по следующим классификационным признакам: *многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается “Служебная тайна” и общедоступная информация:* a) 2Б b) 2А c) 1Г d) 1Д
10.	Методы и средства защиты информации бывают: a) Технические (аппаратные) b) Программные c) Прикладные d) Организационные
11.	Информация по категории доступа классифицируется как: a) Конфиденциальная b) Общедоступная c) Особо конфиденциальная d) Ограниченного доступа
12.	Уязвимость это: a) Совокупность действий, направленная на преодоление системы защиты b) Злонамеренное внедрение специального ПО c) Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации. d) Результат действия вируса
13.	Прерывание это: a) временное прекращение процесса b) остановка процесса

	c) временное прекращение процесса, вызванное событием, внешним по отношению к этому процессу, и совершенное таким образом, что процесс может быть продолжен d) событие, при котором меняется нормальная последовательность команд, выполняемых процессором
14.	Что такое тупиковая ситуация для процесса? a) невозможность выделения процессу требуемого ресурса b) ситуация когда процесс ожидает некоторого события, которое никогда не произойдет c) прерывание процесса операционной системой d) критическая системная ошибка во время выполнения процесса
15.	В каком порядке задаются права доступа в ОС Linux? a) группа-владелец- остальные b) владелец-группа-остальные c) остальные-владелец-группа d) остальные-группа-владелец
16.	Что такое ACL? a) средство для хранения паролей b) сценарий входа в систему c) список управления доступом d) инструмент мандатного управления доступом в ОС
17.	Что из перечисленного не содержится в маркере доступа пользователя? a) идентификатор пользователя b) привилегии пользователя c) идентификатор сеанса работы пользователя, к которому относится маркер доступа d) уровень доступа пользователя в системе
18.	Какова должна быть минимальная длина пароля в случае смены ежеквартально? a) 13 символов b) 12 символов c) 8 символов d) 6 символов
19.	Что из перечисленного не является требование к подсистеме регистрации и учета: a) использование идентификационного и аутентификационного механизма b) запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.) c) обеспечение доверенной загрузки ОС d) действия по изменению ПРД

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ИНДИВИДУАЛЬНЫХ ЗАДАНИЙ

по дисциплине

«Управление информационной безопасностью»

(наименование дисциплины)

1. Международные стандарты в сфере управления информационной безопасностью.
2. Программные и программно-аппаратные средства защиты информации.
3. Программные средства автоматизации процедур проведения аудита информационной безопасности и анализа политики информационной безопасности.
4. Программные средства поддержки процессов управления информационной безопасностью.

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 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 индивидуального задания (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.

Критерии оценки практических занятий

«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.

Критерии оценивания зачета с оценкой

Критерии оценок 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 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.

Формат сведений о ФОС и ее согласовании

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

Б1.Б.32 «Управление информационной безопасностью»
(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./