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)

«ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

(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
(наименование)

Кафедра: Информационная безопасность
(наименование)

Калининград 2018

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Б1.Б.27 «Техническая защита информации»
(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. Концепция инженерно-технической защиты информации.	ОПК-8, ПК-1	собеседование, доклад		устный
2	РАЗДЕЛ 2. Теоретические основы инженерно-технической защиты информации.	ОПК-8, ПК-1, ПК-14, ПК-16, ПК-17	коллоквиум, доклад		устный
			реферат		письменный
			защита лабораторного практикума		письменный
3	РАЗДЕЛ 3. Технические средства добывания и инженерно-технической защиты информации.	ОПК-8, ПК-1, ПК-3, ПК-14, ПК-16, ПК-17	коллоквиум, доклад		устный
			реферат		письменный
			защита лабораторного практикума		письменный
4	РАЗДЕЛ 4. Организационные основы инженерно-технической защиты информации.	ОПК-8, ПК-1, ПК-3, ПК-14, ПК-16, ПК-17	реферат		письменный
			защита лабораторного практикума		письменный
			тестирование		письменный

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.27 «Техническая защита информации»
(код) (наименование дисциплины)

№ п/п	Код компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины студенты должны:		
			знать	уметь	владеть
1.	ОПК-8	способность к освоению новых образцов программных, технических средств и информационных технологий	принципы построения и функционирования, основы теории электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	применять типовые программные средства сервисного назначения; проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; применять на практике методы анализа электрических цепей; работать с современной элементной базой электронной аппаратуры	навыками обеспечения безопасности информации с помощью типовых программных средств; навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы
2.	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	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
3.	ПК-3	способностью проводить анализ защищенности автоматизированных систем	технические каналы утечки информации возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации	анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности автоматизированных систем.	методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

4.	ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	основные информационные технологии, используемые в автоматизированных системах	контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами расчета и инструментального контроля показателей технической защиты информации; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
5.	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	возможности технических средств перехвата информации; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации
6.	ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации

ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Б1.Б.27 «Техническая защита информации»
(код) (наименование дисциплины)

Семестр VII

№ 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
		Этапы формирования компетенции																
1.	ОПК-8	+		+	+									+				
2.	ПК-1	+		+	+			+	+				+	+				
3.	ПК-3		+		+	+	+		+						+	+		+
4.	ПК-14									+	+	+			+			
5.	ПК-16												+	+	+		+	
6.	ПК-17									+	+	+				+	+	+

ПОКАЗАТЕЛИ И КРИТЕРИИ ОПРЕДЕЛЕНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Код контролируемой компетенции (или ее части)	Уровни сформированности компетенции		
	пороговый	продвинутый	высокий
ОПК-8, ПК-1, ПК-3, ПК-14, ПК-16, ПК-17	Знать:		
	Обладает базовыми общими знаниями	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости
	Уметь:		
	Обладает основными умениями, требуемыми для выполнения простых задач	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем
	Владеть:		
	Работает при прямом наблюдении	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем	Контролирует работу, проводит оценку, совершенствует действия работы

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 рабочей тетради и ее тематика определяется кафедрой. Она бывает вызвана, например, наличием труднодоступных для студента, но очень важных для осмысления проблем дисциплины источников. Кафедра может обеспечить студенту возможность работы с этими источниками, опубликовав их в составе рабочей тетради с соблюдением установленных правил такой публикации и снабдив вопросами и заданиями. Как показывает практика, формат тетради весьма удобен для решения студентами конкретных ситуаций, задач. В этом случае работа студента способствует выработке необходимых практических навыков, предусмотренных требованиями к уровню подготовки по данной дисциплине.	Образец рабочей тетради

Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а так же собственные взгляды на неё.	Темы рефератов
Доклад, сообщение	Доклад – это краткое публичное устное изложение результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. 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 учебный материал.	Вопросы на экзамен

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

Типовые вопросы к экзамену

Дисциплина:	Техническая защита информации	Специальность:	10.05.03.
Семестр:	VII		
Кафедра:	Информационная безопасность		

1.	Классификация каналов связи.
2.	Классификация электромагнитных излучений по диапазонам частот и длинам волн согласно номенклатуре международного Регламента радиосвязи.
3.	Характеристика проводных электрических линий связи.
4.	Параметры линий связи.
5.	Помехи (наводки), возникающие в каналах связи.
6.	Характеристика электромагнитных каналов утечки информации.
7.	Характеристика спектральных составляющих ПЭМИН персонального компьютера.
8.	Характеристика электрических каналов утечки информации.
9.	Средства и способы съема информации по электрическим каналам информации.
10.	Классификация демаскирующих признаков объектов.
11.	Характеристика демаскирующих признаков объектов в видимом диапазоне электромагнитного спектра.
12.	Характеристика демаскирующих признаков объектов в инфракрасном диапазоне электромагнитного спектра.
13.	Основные характеристики радиосигналов демаскирующих признаков радиоэлектронных средств.
14.	Классификация технических признаков радиоизлучений.
15.	Классификация демаскирующих признаков акустических закладок.
16.	Основные характеристики микрофонов.
17.	Назначение, состав и принцип работы параболического микрофона.
18.	Назначение, состав и принцип работы плоских фазированных решеток.
19.	Назначение, состав и принцип работы трубчатого микрофона.
20.	Назначение, состав и принцип работы градиентного микрофона.
21.	Основные характеристики направленных микрофонов.
22.	Назначение, решаемые задачи и составные части радиомикрофонов.
23.	Основные тактико-технические характеристики сканирующих радиоприемников.
24.	Назначение, решаемые задачи, ТТХ и принцип работы портативного измерителя частоты MFP-8000.
25.	Основные способы контроля и прослушивания телефонных каналов связи.
26.	Принцип реализации способа прослушивания помещений через микрофон телефонного аппарата (схема прослушивания способом высокочастотного навязывания).
27.	Основные задачи охраны и принципы обеспечения безопасности объектов.
28.	Сформулировать основные особенности построения периметровой системы охраны особо важных объектов.
29.	Реализация периметровой охраны особо важных объектов путем создания функциональных зон.

30.	Оптимизация построения системы охранной безопасности.
31.	Организация контроля доступа к защищаемым помещениям.
32.	Характеристика активных лучевых инфракрасных систем охраны.
33.	Характеристика пассивных инфракрасных систем охраны.
34.	Назначение и составные части оптоволоконных систем охраны.
35.	Особенности реализации охраны периметров с помощью емкостных систем.
36.	Назначение, принцип действия вибрационных систем с сенсорными кабелями.
37.	Назначение, составные части и принцип работы вибрационно-сейсмических систем.
38.	Назначение, устройство и принцип действия радиолучевых систем охраны объектов.
39.	Назначение, принцип действия специальных систем наблюдения за территорией охраняемого объекта.
40.	Особенности реализации защиты электронных устройств с помощью экранирования электромагнитных волн.
41.	Классификация помехоподавляющих фильтров, их амплитудно-частотные характеристики.
42.	Методика расчета параметров LC-фильтров.
43.	Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании.
44.	Назначение, характеристики и принцип работы нелинейного локатора.
45.	Раскрыть особенности функционирования технических средств радиомониторинга и обнаружения закладных устройств.
46.	Раскрыть содержание методики защиты от утечки за счет микрофонного эффекта.
47.	Раскрыть содержание организационных мер защиты информации от утечки за счет электромагнитного излучения.
48.	Раскрыть содержание методики защиты от утечки в волоконно-оптических линиях и системах связи.
49.	Раскрыть содержание основных способов несанкционированного доступа к источникам конфиденциальной информации.
50.	Раскрыть содержание основных способов коммуникации сигналов от закладных микрофонов.
51.	Раскрыть содержание основных способов противодействия подслушиванию телефонных переговоров.
52.	Организация выявления возможных точек расположения лазерного регистратора.
53.	Организация технической защиты от лазерного подслушивания.
54.	Раскрыть содержание способа несанкционированного получения информации за счет приема электромагнитных сигналов радиодиапазона, на примере частной модели радиоперехвата.
55.	Методика определения вероятности установления информационного контакта.
56.	Классифицировать основные методы защиты от радиоперехвата.

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, самостоятельного изучения раздела/темы/вопроса/части вопроса и т.д., консультирования с преподавателем. 3. Особое внимание следует уделить повторению основных понятий и определений дисциплины, а также ключевым моментам изучаемых концепций.
Коллоквиум/ собеседование	Этапы проведения коллоквиума 1. Подготовительный этап: - формулирование темы и проблемных вопросов для обсуждения; - предоставление списка дополнительной литературы; - постановка целей и задач занятия; - разработка структуры занятия; - консультация по ходу проведения занятия;

	2. Начало занятия: - подготовка аудитории: поскольку каждая микрогруппа состоит из 5 - 7 студентов, то парты нужно соединить по две, образовав квадрат, и расставить такие квадраты по всему помещению. - комплектация микрогрупп. - раздача вопросов по заданной теме для совместного обсуждения в микрогруппах. 3. Подготовка учащихся по поставленным вопросам. 4. Этап ответов на поставленные вопросы: - 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

ТЕМЫ ДЛЯ КОЛЛОКВИУМОВ, СОБЕСЕДОВАНИЯ

по дисциплине «Техническая защита информации»
(наименование дисциплины)

1. Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.

2. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.

3. Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.

4. Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем.

5. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.

6. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

7. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.

8. Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов. Модели злоумышленников.

9. Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

10. Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Источники побочных излучений, их физическая природа. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызыва-

ющие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

11. Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах.

12. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.

13. Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

14. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания.

15. Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

16. Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.

17. Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

18. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

19. Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

20. Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

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)»

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

ТЕМЫ РЕФЕРАТОВ, ДОКЛАДОВ

по дисциплине «Техническая защита информации»
(наименование дисциплины)

1. Виды угроз безопасности информации.
2. Основные параметры системы защиты информации.
3. Распространение сигналов в технических каналах утечки информации.
4. Физические процессы подавления опасных сигналов.
5. Физические основы побочных электромагнитных излучений и наводок.
6. Защита информации в компьютерных системах от утечки по каналам ПЭМИН.
7. Основы защиты информации от фотографической и оптико-электронной разведок.
8. Основы защиты информации от радиотехнической разведки.
9. Процессы подавления опасных сигналов.
10. Основные определения и классификация радиоэлектронных помех.
11. Методы и средства инженерной защиты и технической охраны объектов.
12. Классификация и характеристика охранных, пожарно-охранных и пожарных извещателей.
13. Технические средства несанкционированного доступа к информации.
14. Направления обеспечения безопасности.
15. Аттестация объектов, лицензирование деятельности по защите информации и сертификации ее средств.
16. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
17. Классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

18. Технические средства для тестирования и контроля систем обеспечения безопасности информации.
19. Принципы моделирования объектов защиты.
20. Стандартизация систем защиты информации.

Критерии оценивания за устное выступление при обсуждении вопроса

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

Критерии оценивания за подготовку реферата

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

Критерии оценивания доклада с презентацией

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

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

Типовые тестовые (или контрольные) задания

Дисциплина:	Техническая защита информации	Специальность:	10.05.03.
Семестр:	VII		
Кафедра:	Информационная безопасность		

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

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

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

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

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

Критерии оценивания выполнения тестирования (контрольного задания)

а) типовые задания к тесту

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

б) критерии оценивания

Критерием оценивания теста является количество правильно 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 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 осуществляется при условии выполнения заданий всех лабораторных занятий, самостоятельной работы, а также результатами проведенной оценки остаточных знаний.

Формат сведений о ФОС и ее согласовании

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

Б1.Б.27 «Техническая защита информации»
(код) (наименование дисциплины)

образовательной программы специалитета по специальности

10.05.03. Информационная безопасность автоматизированных систем

специализация программы

Обеспечение информационной безопасности распределенных информационных систем

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./