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_» _июня_ 20_18_ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

(приложение к рабочей программе дисциплины)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины)

вариативной части дисциплина специализации образовательной программы специалитета

25.05.03. "Техническая эксплуатация транспортного радиооборудования"
(код и наименование направления)

Специализация программы

"Инфокоммуникационные системы на транспорте и их информационная защита"
(наименование специализации)

Факультет: Радиотехнический
(наименование)

Кафедра: Информационная безопасность
(наименование)

Калининград 2018

Содержание

1.	Результат освоения дисциплины.		3
2.	Перечень оценочных средств.		5
3.	Оценочные средства поэтапного формирования результатов освоения дисциплины.		5
3.	3.1.	Типовые контрольные задания и вопросы, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций. Описание оценочных средств.	5
	3.2	Методические материалы, определяющие процедуры использования оценочных средств (в том числе показатели, критерии и шкалы оценивания результатов освоения дисциплины).	11
4	Оценочные средства для итоговой аттестации и критерии оценки итоговой компетенции по дисциплине		14
	4.1	Типовые экзаменационные вопросы	16
	4.2	Критерии оценок итогового уровня знаний и умений по дисциплине	17
5.	Сведения о фонде оценочных средств и его согласовании.		19

1 Результат освоения дисциплины.

Дисциплина «Основы информационной безопасности» изучается в седьмом семестре. Процесс изучения дисциплины заканчивается экзаменом.

Компетенции, закреплённые за дисциплиной «Основы информационной безопасности» в ОП ВО по специальности 25.05.03 «Техническая эксплуатация транспортного радиооборудования»: Специализация: Инфокоммуникационные системы на транспорте и их информационная защита»

Наименование этапа	**Код и наименование компетенции**		
ОПК-5.1: Способность использовать основные методы, способы и средства получения, хранения, переработки информации; ОПК-5.2: Способность работать с компьютером как средством управления информацией.			
	Знать	Уметь	Владеть
Этап «текущей аттестации»	по месяцам аттестации		
	Знания, умения и навыки при формировании компетенции на данном этапе оцениваются в соответствии с Положением о текущей аттестации		
Этап «промежуточной (семестровой) аттестации»	сущность и понятие информационной безопасности, актуальность проблемы информационной безопасности; характеристику составляющих ИБ, основные проблемы защиты информационно-технологических ресурсов организации; средства и методы обеспечения информационной безопасности;; концептуальные подходы к обеспечению информационной безопасности;	составлять аналитические обзоры по вопросам обеспечения ИБ автоматизированных систем; определять комплекс мер для обеспечения ИБ автоматизированных систем; исследовать компьютерные модели автоматизированных систем безопасности	профессиональной терминологией в области информационной безопасности; методами учета и обработки информации; методами формирования требований по защите информации.
ОПК-6.2: Способность сознавать опасности и угрозы, возникающие в развитии современного информационного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны			
	Знать	Уметь	Владеть
Этап «текущей	по месяцам аттестации		

аттестации»	Знания, умения и навыки при формировании компетенции на данном этапе оцениваются в соответствии с Положением о текущей аттестации		
Этап «промежуточной (семестровой) аттестации»	основные отечественные и зарубежные стандарты в области информационной безопасности; место и роль информационной безопасности в системе национальной безопасности РФ; основы государственной информационной политики, стратегию развития информационного общества в России.	использовать 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 обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.	навыками работы с нормативными правовыми актами в области защиты информации; навыками постановки и решения задачи обеспечения информационной безопасности компьютерных систем; навыками управления информационной безопасностью.
ПСК-2.5.1: Способность эксплуатировать системы обеспечения информационной безопасности телекоммуникационных систем; ПСК-2.5.2: Способность эксплуатировать средства обеспечения информационной безопасности телекоммуникационных систем.			
	Знать	Уметь	Владеть
Этап «текущей аттестации»	по месяцам аттестации		
	Знания, умения и навыки при формировании компетенции на данном этапе оцениваются в соответствии с Положением о текущей аттестации		
Этап «промежуточной (семестровой) аттестации»	принципы формирования политики информационной безопасности в телекоммуникационных и автоматизированных системах; алгоритмы шифрования информации и аутентификации пользователей; методы и средства ТЗИ	проводить мониторинг угроз безопасности телекоммуникационных систем; разрабатывать модели угроз и нарушителей ИБ автоматизированных систем; применять знания о системах электрической связи для решения задач по созданию защищённых телекоммуни-	методами формирования требований по защите информации; навыками использования программно-аппаратных средств обеспечения ИБ автоматизированных систем; методами и средствами тзи

		кационных систем	

2 Перечень оценочных средств.

Рабочая программа обеспечена фондом оценочных средств, для проведения текущего контроля и промежуточной аттестации. К оценочным средствам поэтапного формирования результатов освоения дисциплины относятся:

-задания в тестовой форме;

-контрольная работа для заочной и заочной ускоренной формы обучения выполняется в реферативной форме

К оценочным средствам для итоговой аттестации по дисциплине относятся экзаменационные вопросы

Фонд оценочных средств представлен в учебно-методическом комплексе дисциплины.

3 . Оценочные средства поэтапного формирования результатов освоения дисциплины

3.1.Типовые контрольные задания и вопросы, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций. Описание оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Тест	Форма контроля, направленная на проверку уровня освоения контролируемого теоретического и лабораторного материала по дидактическим единицам дисциплины (терминологический аппарат, основные методы, ИТ, приёмы, документы. Компьютерные программы, используемые в изучаемой области).	Фонд тестовых заданий

2	Контрольная работа (СРС)	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определённой учебно-исследовательской темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на неё.	Фонд вопросов по СРС, фонд тем контрольных работ в реферативной форме
3	Экзамен	Экзамен служит формой проверки качества усвоения учебного материала в соответствии с утверждённой программой	Фонд экзаменационных вопросов

Наименование этапа	Вид оценочного средства
Этап «текущей аттестации»	Тест, Лабораторные работы, Контрольная работа (СРС)
Этап «промежуточной (семестровой) аттестации»	Экзамен: экзаменационные вопросы

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенций или её части		Оценочные средства-наименования	
				Текущий контроль	Промежуточная итоговая аттестация
Аттестация 1					
1.	Раздел 1. Информационная безопасность в системе национальной безопасности РФ	ОПК-6.2	Знать Уметь Владеть	Выполнение лабораторной работы.	Вопросы к экзамену
Аттестация 2.					
2.	Раздел 2. Виды информации, методы и средства обеспечения ИБ. Анализ угроз ИБ.	ОПК-5.1 ОПК-5.2	Знать Владеть Уметь	Выполнение лабораторной работы контрольная работа в реферативной форме.	Вопросы к экзамену
Аттестация 3					
		ПСК-	Знать	Выполнение ла-	Вопросы к

3	Раздел 3. Защита информации	2.5.1	Уметь	бораторной работы, тест	экзамену
		ПСК-2.5.2	Владеть		

3.1.1 Типовые тестовые задания.

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

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

19.	Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем **б) объективных проблем современной технологии программирования** в) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы г) постоянные атаки хакеров
20.	В число принципов управления персоналом входит: а) разделяй и властвуй **б) разделение обязанностей** в) метод кнута и пряника г) разделение доступа
21.	Меры информационной безопасности направлены на защиту от: а) **нанесения неприемлемого ущерба** б) нанесения любого ущерба в) подглядывания в замочную скважину г) нанесения морального вреда
22.	На межсетевые экраны целесообразно возложить следующие функции: а) **антивирусный контроль "на лету"** б) антивирусный контроль компьютеров внутренней сети в) антивирусный контроль компьютеров внешней сети г) антивирусный контроль всех съемных носителей
23.	На современном этапе развития законодательного уровня информационной безопасности в России важнейшее значение имеют: а) меры ограниченной направленности б) **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

3.1.2 Типовые темы контрольной работы

1. Классифицировать информационные ресурсы, определить свойства классификационных групп.
2. Дать определение информационной безопасности и проанализировать ее цели, задачи и структуру.
3. Проанализировать содержание концепции информационной безопасности.
4. Обосновать необходимость информационной безопасности человека и общества.
5. Определить место информационной безопасности в структуре информационного права.
6. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.
7. Дать определение информационным ресурсам, охарактеризовать их основные свойства, взаимосвязь с материальными и иными ресурсами.
8. Проанализировать правовые и экономические предпосылки охраны интеллектуальной собственности и защиты предпринимательской информации.
9. Описать порядок охраны информационных ресурсов открытого доступа.
10. Охарактеризовать порядок защиты информационных ресурсов ограниченного доступа.
11. Выявить соотношение понятий ценности, полезности и достоверности информационных ресурсов.
12. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
13. Понятие конфиденциальности, дать его определение, классификацию конфиденциальной информации по объектам владения.
14. Дать классификацию источников конфиденциальной информации, охарактеризовать каждый источник.
15. Обосновать сущность разведки в бизнесе, легальных методов получения ценной информации.
16. Дать классификацию нелегальных методов промышленного шпионажа.
17. Дать классификацию каналов объективного распространения конфиденциальной информации.
18. Определить сущность несанкционированного канала утраты конфиденциальной информации.
19. Классифицировать организационные каналы утраты конфиденциальной информации.
20. Классифицировать технические каналы утраты конфиденциальной информации.
21. Показать соотношение организационных и технических каналов утраты информации в компьютерах и локальных сетях.
22. Обосновать необходимость защиты информационных ресурсов от несанкционированного доступа.
23. Концептуальные особенности защиты информации, ее органическая связь с информационной безопасностью.
24. Обосновать структуру системы защиты информации, охарактеризовать ее комплексность.

25. Определить понятие угрозы информации, классифицировать угрозы по различным основаниям.
26. Назначение и содержание правового элемента системы защиты.
27. Назначение и содержание организационного элемента системы защиты.
28. Назначение и содержание инженерно-технического элемента системы защиты.
29. Назначение и содержание программно-аппаратного элемента системы защиты.
30. Назначение и содержание криптографического элемента системы защиты.
31. Критерии формирования системы защиты в зависимости от ценности информации, размера прибыли или убытков и стоимости системы защиты.
32. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
33. Дать соотношение понятий "допуск" и "доступ" к конфиденциальной информации.
34. Обосновать принципы практической реализации системы доступа персонала к конфиденциальной информации.
35. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.
36. Сравнить способы учета конфиденциальных документов, изготовленных на дискете, выявить критерии определения эффективности каждого из способов.
37. Сравнить способы учета электронных конфиденциальных документов, передаваемых по линии защищенной компьютерной связи, выявить критерии определения эффективности каждого из способов.
38. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети проанализировать степень опасности каждого канала.
39. Составить схему рекомендуемых рубежей охраны фирмы и проанализировать эффективность системы охраны.
40. Проанализировать сферы использования различных направлений и методов аналитической работы по выявлению каналов утраты конфиденциальной информации.
41. Графически (схематически) описать технологию выполнения процедур и операций конкретной части того или иного элемента системы защиты информации (по выбору преподавателя).
42. Проанализировать ситуационный вариант и выработать меры противодействия угрозам конфиденциальной информации.
43. Скремблирование информации.

3.2 Методические материалы, определяющие процедуры использования оценочных средств (в том числе показатели, критерии и шкалы оценивания результатов освоения 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 курсанта(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 курсанта (студента) к лекции в первую очередь предполагает повторение законспектированного материала предыдущей лек-

	ции. 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 курсантов (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.
Лабораторные 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, и др.
Контрольная работа	Написание контрольной работы в реферативной форме условно разделяется на два этапа: подготовительный и основной; теоретический и практический. На первом этапе курсант (студент) определяется с темой исследования: А) Преподаватель распределяет темы лично (учитывая ваши возможности и способности). Б) Курсанту (студенту) предоставляется право выбора темы из списка, составленного преподавателем. В) Курсант (студент) может самостоятельно придумать тему для своей контрольной работы 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 вашей контрольной работы в реферативной форме. 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. Контрольная работа обычно составляет 8-16 страниц, иногда изложение может составлять до 20 страниц текста. Традиционно оно состоит из таких блоков: • Титульный лист. • План работы. • Введение. • Общее изложение темы. • Заключение. • Перечень использованных литературных источников. Чтобы грамотно составить доклад следует более подробно остановиться на каждом пункте. Титульный лист. 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 контрольной работы в реферативной форме. Раздел Введения строится по аналогии с курсовой ра-

	ботой 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 контрольной работы 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 работы 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.

3.2.1 На этапе «текущей аттестации» при защите письменных отчётов по лабораторным работам применяется следующая шкала оценивания обучающихся.

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 процессов, исследовать их и вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения объектов, систем, процессов;
- владение навыками работы с пакетами прикладных программ для моделирования и анализа 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.

3.2.2 Критерии оценивания выполнения контрольной работы в реферативной форме.

5 «Отлично»	выполнены все требования к написанию и защите контрольной работы в реферативной форме: 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 выполнению контрольной работы в реферативной форме и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём контрольной работы; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
3 «Удовлетворительно»	имеются существенные отступления от требований к выполнению контрольной работе в реферативной форме. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании контрольной работы или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
2 «Неудовлетворительно»	тема контрольной работы в виде реферата не раскрыта, обнаруживается существенное непонимание проблемы.

3.2.3 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%.

4 Оценочные средства для итоговой аттестации и критерии оценки итоговой компетенции по дисциплине

№ п/п	Код контролируемой компетенции	Уровни сформированности компетенций

	(или ее части)	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (Отлично)
1	ОПК-6.2	Знать:		
		основные отечественные и зарубежные стандарты в области информационной безопасности;	Место и роль ИБ в системе национальной безопасности РФ	Основы государственной информационной политики, стратегию развития информационного общества в России
		Уметь:		
		Использовать 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 обеспечения ИБ	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
		Владеть:		
		Навыками работы с нормативными правовыми актами в области защиты информации	Навыками постановки и решения задач обеспечения ИБ компьютерных систем	Навыками управления ИБ
2	ОПК-5.1	Знать:		
		Сущность и понятие ИБ, актуальность проблемы ИБ	Характеристику составляющих ИБ, основные проблемы защиты информационно-технологических ресурсов организации	Средства и методы обеспечения информационной безопасности, концептуальные подходы к обеспечению ИБ
	ОПК-5.2	Уметь:		
		Составлять аналитические обзоры по вопросам обеспечения ИБ автоматизированных систем	Определять комплекс мер для ИБ автоматизированных систем	Исследовать компьютерные модели автоматизированных систем безопасности
	ОПК-5.1.	Владеть:		
		Профессиональной терминологией в области ИБ	Методами учёта и обработки информации	Методами формирования требований по защите информации
3	ПСК-2.5.1	Знать:		
		Принципы формирования политики ИБ в телекоммуникационных и автоматизированных системах	Алгоритмы шифрования информации и аутентификации пользователей	Методы и средства ТЗИ
		Уметь:		

		Проводить мониторинг угроз безопасности телекоммуникационных систем	Разрабатывать модели угроз и нарушителей ИБ автоматизированных систем	Применять знания о системах электрической связи для решения задач по созданию защищённых телекоммуникационных систем
	ПСК-2.5.2	Владеть:		
		Методами формирования требований по защите информации	Навыками использования программно-аппаратных средств обеспечения ИБ автоматизированных систем	Методами и средствами ТЗИ

4.1 Типовые экзаменационные вопросы.

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

25.	Способы защиты информации в локальных и глобальных компьютерных сетях.
26.	Основные виды технических каналов и источников утечки информации в автоматизированных системах.
27.	Физические основы утечки защищаемой информации по акустическому каналу, линиям связи и каналу побочного электромагнитного излучения.
28.	Характеристики каналов утечки информации в автоматизированных системах.
29.	Способы предотвращения утечки информации по техническим каналам.
30.	Классификация средств вычислительной техники по защищенности от НСД.
31.	Классификация автоматизированных систем по защищенности от НСД.
32.	Классификация межсетевых экранов по защищенности от НСД.
33.	Обобщенная схема обеспечения информационной безопасности. Структура унифицированной концепции защиты информации.
34.	Классификация (критерии) технических средств защиты информации.
35.	Общие принципы создания и функционирования системы обеспечения безопасностью предприятия.
36.	Назначение политики безопасности и ее содержание.
37.	Этапы создания систем защиты информации.
38.	Назначение и функции службы безопасности предприятия.
39.	Содержание деятельности службы безопасности.
40.	Типовая структура службы безопасности предприятия. Обязанности сотрудников.
41.	Система стандартов в области защиты информации.
42.	Основное содержание стандарта ISO27001 (17799):2005. Результаты работы предприятия по подготовке к сертификации по стандарту.
43.	Основы проектирования и оценка систем физической защиты. Последовательность и содержание работ по проектированию систем физической защиты.
44.	Основное содержание Протокола обследования предприятия.
45.	Основное содержание отчета об оценке анализа уязвимости предприятия.
46.	Определение и место информационной безопасности в общей совокупности информационных проблем современного общества.
47.	Законодательная база Российской Федерации по обеспечению информационной безопасности.
48.	Международные нормативно-правовые акты в области информационной безопасности.

4.2 Критерии оценок итогового уровня знаний и умений по дисциплине

Экзамен по дисциплине проводится при условии выполнения заданий всех лабораторных занятий, контрольной работы в реферативной форме, а также результатами проведенной оценки знаний в виде теста.

Неудовлетворительный	Пороговый	Углублённый	Продвинутый
«2» (неудовлетв.)	«3» (удовлетвор.)	«4» (хорошо)	«5» (отлично)

Не раскрыто содержание вопроса, не использован основной материал, не раскрыта суть понятий и категорий, отсутствие понимания темы вопроса и дисциплины в целом. Пропуски лекций, лабораторных занятий, не выполненное тестовое задание, реферат. Не может ответить на дополнительные вопросы по пройденному материалу	Дана краткая, неглубоко осмысленная характеристика темы, использован не весь материал, раскрывающий сущность явления	Точно дана общая характеристика вопроса, обозначены основные понятия и персоналии, сделаны выводы.	Дан развёрнутый, аргументированный ответ, в котором подробно изложена тема вопроса, раскрыты причинно-следственные связи, верно определены научные термины и понятия, показан необходимый уровень обобщения и осмысления материала. Показано умение анализировать различные точки зрения. Приведён полный фактический материал, раскрывающий содержание вопроса. Раскрыты компетенции, имеющие отношение к данному вопросу.

Формат сведений о ФОС и ее согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Основы информационной безопасности» образовательной программы специалитета по специальности **25.05.03.** "Техническая эксплуатация транспортного радиооборудования» Специализация программы "Инфокоммуникационные системы на транспорте и их информационная защита" утвержденной «21» 06 2018 г.

Авторы фонда – доцент кафедры ИБ Великите Н.Я., и.о. декана РТФ Баженов В.А.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «ИБ» (протокол №9 от 14.06 2018 г.)

И.о. декана РТФ _____/Баженов В.А./

Заведующий кафедрой ИБ _____/Великите Н.Я./

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

(протокол №6 от 07.06 2018 г.)

Председатель методической комиссии РТФ _____/Жестовский А.Г./

Согласовано

Начальник отдела мониторинга и контроля

_____/Борисевич Ю.В./