	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»		стр. 1 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

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

УТВЕРЖДАЮ
И.о. декана радиотехнического факультета

/В.А. Баженов/
27.10.2018 г.



Рабочая программа дисциплины
Основы информационной безопасности
(наименование дисциплины)


вариативной части дисциплина специализации образовательной программы специалитета
по специальности

25.05.03 «Техническая эксплуатация транспортного радиооборудования»
(код и наименование специальности)

Специализация
«Инфокоммуникационные системы на транспорте и их информационная защита»
(наименование профиля программы)

Радиотехнический факультет
(наименование)
Кафедра информационной безопасности
(наименование)

Калининград 2018 г.

	Балтийская государственная академия рыбопромыслового флота	стр. 2 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»	
	Рабочая программа дисциплины «Основы информационной безопасности»	
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« 07 » 06 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « 07 » 06 2018 г. № 9

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году


Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

	Балтийская государственная академия рыбопромыслового флота		стр. 3 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

1 Цель освоения дисциплины

1.1 Цель изучения дисциплины

Целью изучения дисциплины является формирование у студентов знаний в области основ информационной безопасности и получение навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

1.2 Задачи изучения дисциплины

К задачам дисциплины относятся изучение современных методов и систем информационной безопасности; ознакомление обучаемых с тенденциями развития защиты информации, сформировать представление в области теоретических основ компьютерной безопасности, познакомить с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации; научить грамотному использованию средств и методов защиты информации в профессиональной деятельности; сформировать целостное понятие информационной защиты организации как совокупности законодательно-правовых, аппаратных и программных средств и методов.


2 Результаты освоения дисциплины

Таблица 1.1 – Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ОПК-5	<p>Способность использовать основные методы, способы и средства получения, хранения, переработки информации, работать с компьютером как средством управления информацией</p> <p>Этапы формирования компетенций: <u>ОПК-5.1:</u> Способность использовать основные методы, способы и средства получения, хранения, переработки информации; <u>ОПК-5.2:</u> Способность работать с компьютером как средством управления информацией.</p>	<p>знать:</p> <ul style="list-style-type: none"> • 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; <p>уметь:</p> <ul style="list-style-type: none"> • составлять аналитические обзоры по вопросам обеспечения ИБ автоматизированных систем • определять комплекс мер для обеспечения ИБ автоматизированных систем • исследовать компьютерные модели автоматизированных систем безопасности

	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»	стр. 4 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»	
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

		<p>владеть:</p> <ul style="list-style-type: none"> • профессиональной терминологией в области информационной безопасности; • методами учета и обработки информации; • методами формирования требований по защите информации.
ОПК-6	<p>Способность понимать сущность и значение информации в развитии современного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны</p> <p>Этапы формирования компетенций: 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</p>	<p>знать:</p> <ul style="list-style-type: none"> • 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. <p>уметь:</p> <ul style="list-style-type: none"> • 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. <p>владеть:</p> <ul style="list-style-type: none"> • 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	Способность эксплуатировать системы и средства обеспечения информационной безопасности телекоммуникационных систем.	<p>Знать:</p> <ul style="list-style-type: none"> • принципы формирования политики информационной безопасности в телекоммуникационных

	Балтийская государственная академия рыбопромыслового флота		стр. 5 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации	25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

	<p>Этапы формирования компетенций:</p> <p><u>ПСК-2.5.1:</u> Способность эксплуатировать системы обеспечения информационной безопасности телекоммуникационных систем;</p> <p><u>ПСК-2.5.2:</u> Способность эксплуатировать средства обеспечения информационной безопасности телекоммуникационных систем.</p>	<p>и автоматизированных системах;</p> <ul style="list-style-type: none"> • алгоритмы шифрования информации и аутентификации пользователей • методы и средства ТЗИ <p>Уметь:</p> <ul style="list-style-type: none"> • 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 <p>Владеть:</p> <ul style="list-style-type: none"> • методами формирования требований по защите информации • навыками использования программно-аппаратных средств обеспечения ИБ автоматизированных систем • методами и средствами тзи
--	--	---

Таблица 1.2 – Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	основные понятия и определения информационной безопасности; нормативно-правовые акты по обеспечению информационной безопасности, используемые в мировом и российском законодательстве; источники, риски и формы атак на информацию; угрозы, которым подвергается информация; классификацию вредоносных программ; модели безопасности компьютерной системы; средства защиты от компьютерных вирусов и других вредоносных программ; стандарты информационной безопасности; криптографические методы и алгоритмы шифрования информации; алгоритмы аутентификации пользователей; методы защиты информации в сетях; требования к системам защиты информации.
уметь	выявлять источники, риски и формы атак на информацию; разрабатывать политику безопасности организации в соответствии со стандартами безопасности; использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей.

	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»		стр. 6 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

владеть	методами обеспечения информационной безопасности на основе выбранной политики безопасности организации в соответствии со стандартами безопасности.
----------------	--

3 Место дисциплины в структуре образовательной программы

3.1 Место дисциплины в структуре ООП специалитета :

Б1.В.04 Вариативная часть. Обязательная дисциплина. Дисциплины специализации. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

3.2 Требования к предварительной подготовке обучающегося:

Для успешного освоения дисциплины студент должен иметь базовую подготовку по следующим дисциплинам (модулям): Информатика и информационные технологии, Организация ЭВМ и систем, Компьютерные сети и Интернет-технологии

3.3 Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее:

Дисциплина (модуль) относится к обязательным дисциплинам базовой части профессионального цикла и является базовой для успешного освоения такой дисциплины (модуля) профессионального цикла как «Сети и системы радиосвязи и средства их информационной защиты».

4 Содержание дисциплины

Раздел 1. Информационная безопасность в системе национальной безопасности РФ.

Тема 1. Введение в предмет.

Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

Тема 2. Основные понятия теории информационной безопасности.


Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Тема 3. Государственная информационная политика.

Определение, сущность и содержание государственной информационной политики. Угрозы информационному обеспечению государственной политики Российской Федерации.

Тема 4. Информационная безопасность в системе национальной безопасности российской федерации.

Принципы обеспечения информационной безопасности. Унифицированная концепция защиты информации. Модели решения слабо структурированных и плохо формализуемых задач.

	Балтийская государственная академия рыбопромыслового флота		стр. 7 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

Тема 5. Организационно-правовое обеспечение информационной безопасности.

Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Правовые режимы защиты информации конфиденциального характера. Правовая охрана результатов интеллектуальной деятельности.

Раздел 2. Виды информации, методы и средства обеспечения информационной безопасности. Анализ угроз ИБ

Тема 6. Виды информации, методы и средства обеспечения информационной безопасности.

Виды информации. Методы и средства обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Информационная безопасность и информационное противоборство.

Тема 7 Анализ угроз информационной безопасности.

Средства поддержки процессов управления информационной безопасностью АС. Политика безопасности автоматизированных систем. Интеллектуальные системы обработки данных и проблемы информационной безопасности в интернет.

Тема 8. Причины, виды, каналы утечки и искажения информации.

Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Основы физической защиты объектов информатизации. Организация технической защиты информации на объектах информатизации.


Раздел 3. Защита информации

Тема 9. Защита информации

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.

Тема 10. Предупреждение нарушений безопасности

Средства поддержки процессов управления информационной безопасностью АС. Политика безопасности автоматизированных систем. Интеллектуальные системы обработки данных и проблемы информационной безопасности в интернет. Стандарты для безопасности электронной коммерции в сети Интернет. Оценка рисков нарушения информационной безопасности.

	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»		стр. 8 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»		
	Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

5 Объём (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 5.1 – Структура дисциплины по очной форме обучения

Семестр - седьмой (144 час, 4 ЗЕТ.)						
Номер и наименование разделов и тем	Объём учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	Контроль	Всего
Раздел 1. Информационная безопасность в системе национальной безопасности РФ.	8	12		29		49
Тема 2. Введение в предмет. Основные понятия теории информационной безопасности	2	4		9		17
Тема 3. Государственная информационная политика	2	2		6		10
Тема 4. Информационная безопасность в системе национальной безопасности РФ	2	2		6		12
Тема 5. Организационно-правовое обеспечение информационной безопасности.	2	4		8		14
Раздел 2. Виды информации, методы и средства обеспечения информационной безопасности. Анализ угроз ИБ	6	12		18		36
Тема 6. Виды информации, методы и средства обеспечения информационной безопасности.	2	2		6		12
Тема 7. Анализ угроз информационной безопасности.	2	6		6		12
Тема 8. Причины, виды, каналы утечки и искажения информации.	2	4		6		12
Раздел 3. Защита информации	4	12		16		32
Тема 9. Защита информации	2	6		8		13
Тема 10. Предупреждение нарушений безопасности	2	6		8		13
Подготовка к сдаче и сдача экзамена					27	27
Итого по дисциплине	18	36		63	27	144



	Балтийская государственная академия рыбопромыслового флота		стр. 9 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

Таблица 5.2 – Структура дисциплины по заочной форме обучения


Курс- пятый (144 час, 4 ЗЕТ.)						
Номер и наименование разделов и тем	Объём учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СРС	Контроль	Всего
Раздел 1. Информационная безопасность в системе национальной безопасности РФ.	2	2		40		44
Тема 1. Информационная безопасность в системе национальной безопасности РФ	1	1		20		22
Тема 2. Организационно-правовое обеспечение информационной безопасности.	1	1		20		22
Раздел 2. Виды информации, методы и средства обеспечения информационной безопасности. Анализ угроз ИБ	6	4		60		74
Тема 3. Виды информации, методы и средства обеспечения информационной безопасности.	2	2		24		28
Тема 4. Анализ угроз информационной безопасности.	2	2		24		28
Тема 5. Причины, виды, каналы утечки и искажения информации.	2			20		22
Раздел 3. Защита информации		2		15		17
Тема 6. Защита информации		2		15		17
Подготовка к сдаче и сдача экзамена					9	9
Итого по дисциплине	8	8		119	9	144

	Балтийская государственная академия рыбопромыслового флота		стр. 10 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

6 Лабораторные занятия (работы)

Таблица 6.1 – Лабораторные работы по очной форме обучения

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов
Семестр – седьмой (29 час.).			
1.	Тема 1.	Информация как объект информационной защиты. Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных. Государственная система правового обеспечения защиты информации в Российской Федерации. Международные стандарты информационной безопасности. Стандарт ISO 17799: Code of Practice for Information Security Management. Стандарт ISO 15408: Common Criteria for Information Technology Security Evaluation. Стандарт SysTrust. Стандарт BSMT Baseline Protection Manual. Стандарт COBIT 3rd Edition. Стандарты SCORE и программа сертификации SANS/GIAC Site Certification. Отечественная нормативная база информационной безопасности.	4
2.	Тема 2.	Работа с основными нормативными руководящими документами, касающимися государственной тайны, нормативно-справочными документами. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	2
3.	Тема 3.	Конституционные основы информационной безопасности личности. Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных. Угрозы компьютерной безопасности при работе в сети Интернет	2
4.	Тема 4.	Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны. Стратегия развития законодательства в сфере обеспечения ИБ. Законодательные основы защиты прав работника и работодателя в процессе обеспечения ИБ предприятия. Юридические аспекты борьбы со спамом.	4
5.	Тема 5.	Методы обработки аналоговой, дискретной и цифровой информации. Парольная защита. Архивирование с паролем. Модели оценки стойкости парольной защиты.	2
6.	Тема 6	Организация защиты файлов текстовых документов средствами текстового редактора MS Word. Организация защиты файлов табличных документов средствами MS Excel. Организация защиты баз данных средствами MS Access.	6
7	Тема 7	Исследование способов защиты информации и устранения уязвимостей. Исследование методов внешней защиты компьютерных сетей с помощью сетевых экранов.	4
8	Тема 8	Элементы криптографии. Симметричный алгоритм шифрования. Корректирующие коды. Защита информации с помощью про	6

	Балтийская государственная академия рыбопромыслового флота		стр. 11 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

		граммного обеспечения. Криптографическая защита информации	
9	Тема 9	Защита от утечки по цепям питания и заземления. Защита информации от утечки за счет электромагнитного излучения. DLP системы.	6
Всего за семестр:			36

Таблица 6.2 – Лабораторные работы по заочной форме обучения

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов
Сессия – F (8 час.)			
1.	Тема 1.	Угрозы компьютерной безопасности при работе в сети Интернет	2
2.	Тема 2.	Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны.	2
3.	Тема 3.	Организация защиты файлов текстовых документов средствами текстового редактора MS Word. Организация защиты файлов табличных документов средствами MS Excel. Организация защиты баз данных средствами MS Access.	2
4.	Тема 4.	Методы обработки аналоговой, дискретной и цифровой информации. Парольная защита. Архивирование с паролем. Модель оценки стойкости парольной защиты	2
5.	Тема 5.	Исследование способов защиты информации и устранения уязвимостей. Исследование методов внешней защиты компьютерных сетей с помощью сетевых экранов.	
6.	Тема 6.	Элементы криптографии. Симметричный алгоритм шифрования. Корректирующие коды. Защита информации с помощью программного обеспечения. Криптографическая защита информации	2
Всего по итогам дисциплины:			10

7 Практические занятия

Практические занятия по дисциплине «Основы информационной безопасности» отсутствуют.

8 Самостоятельная работа студента

Изучение теоретического материала по учебникам и учебным пособиям; подготовка к лабораторным занятиям (оформление отчетов по лабораторным работам).


	Балтийская государственная академия рыбопромыслового флота		стр. 12 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

Таблица 8.1 – Самостоятельная работа студента по очной форме обучения


№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации	
Семестр – седьмой 63 (час.)				
1.	Международные стандарты информационного обмена.	6	Текущий контроль: Собеседование по СРС, тест	
2.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	6		
3.	Определение, сущность и содержание государственной информационной политики. Угрозы информационному обеспечению государственной политики Российской Федерации.	6		
4.	Принципы обеспечения информационной безопасности. Унифицированная концепция защиты информации. Модели решения слабо структурированных и плохо формализуемых задач.	6		
5.	Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Создание системы информационной безопасности предприятия. Правовые нормы защиты информации в автоматизированных системах.	6		
6	Виды возможных нарушений информационной системы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов. Методы обработки аналоговой, дискретной и цифровой информации.	6		Текущий контроль: Собеседование по СРС
7	Понятие угрозы. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.	6		
8	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Аттестация объектов, лицензирование деятельности по защите информации и сертификации ее средств. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классифика-	6		

	Балтийская государственная академия рыбопромыслового флота		стр. 13 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации	25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

	ция и возможности.		
9	Особенности инструментального контроля эффективности инженерно-технической защиты информации. Защита АС и СВТ от внешнего электромагнитного воздействия. Скремблирование информации. Методы криптографии	8	
10	Тенденции развития теории и практики компьютерной безопасности. DLP системы, технологии предотвращения утечек конфиденциальной информации из ИС.	7	
Итого за семестр		63	

Таблица 8.2 – Самостоятельная работа студента по заочной форме обучения

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Курс – пятый (119 час.).			
1.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Определение, сущность и содержание государственной информационной политики. Угрозы информационному обеспечению государственной политики Российской Федерации.	20	Текущий контроль: собеседование, тест
2.	Принципы обеспечения информационной безопасности. Унифицированная концепция защиты информации. Модели решения слабо структурированных и плохо формализуемых задач. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Создание системы информационной безопасности предприятия. Правовые нормы защиты информации в автоматизированных системах.	20	
3.	Виды возможных нарушений информационной системы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов. Методы обработки аналоговой, дискретной и цифровой информации.	20	
4.	Понятие угрозы. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России	20	


	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»		стр. 14 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»		
	Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»	

5.	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.	20	
6.	Особенности инструментального контроля эффективности инженерно-технической защиты информации. Защита АС и СВТ от внешнего электромагнитного воздействия. Скремблирование информации. Методы криптографии. Тенденции развития теории и практики компьютерной безопасности. DLP системы, технологии предотвращения утечек конфиденциальной информации и ИС	19	
Всего по дисциплине		119	

9 Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

Таблица 9.1 – Основная учебная литература

№ п/п	Автор(ы)	Заглавие	Город, издательство, год издания,
1	Куприянов А.И., Сахаров А.В.	Основы защиты информации: Учебное пособие	М.: Академия, 2008 (наличие в библиотеке БГАРФ - 31 экз.)
2	Расторгуев С.П.	Основы информационной безопасности: Учебное пособие	М.: Академия, 2007. (наличие в библиотеке БГАРФ - 20 экз.)
3	В. П. Мельников, С. Я. Клейменов, А. М. Петраков	Информационная безопасность и защита информации [Текст] : учебное пособие /. - 3-е изд..	М.: Изд. центр "Академия", 2008 (наличие в библиотеке БГАРФ - 31 экз.)
4	Шаньгин, В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум: Инфра-М, 2010. – 415 с. (наличие в библиотеке БГАРФ - 15 экз.)
5	Кузнецов, А.В	Основы защиты информации : учеб. пособие для студентов	БГАРФ, 2014. – 122 с. (наличие в библиотеке

	Балтийская государственная академия рыбопромыслового флота		стр. 15 из 19
	ФГБОУ ВО «Калининградский государственный технический университет»		
	Рабочая программа дисциплины «Основы информационной безопасности»		
Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»		

		ресурсе]	2011. – 288 с. – Режим доступа: http://www.iprbookshop.ru/11979
2	Соколов, М. С.	Информация как объект информационной безопасности [Электронный ресурс]	Закон и право. – 2013. – №12. – С.27-33. – Режим доступа: http://elibrary.ru/item.asp?id=20780302
3	Сычев Ю. П.	Основы информационной безопасности [Электронный ресурс]	учеб.-практ. пособие / Ю. П. Сычев. – Электрон. текстовые дан. – Москва: ИАОИ, 2010. – 328 с. – Режим доступа: http://www.iprbookshop.ru/10746
4	Е. Б. Белов	Основы информационной безопасности [Электронный ресурс]	учеб. пособие для вузов / Е. Б. Белов [и др.]. – Электрон. текстовые дан. – М.: Горячая линия-Телеком, 2011. – 544 с. – Режим доступа: 25 http://www.iprbookshop.ru/12014.html

10 Информационные технологии, программное обеспечение и интернет-ресурсы дисциплины

10.1 Информационные технологии

Электронная информационная образовательная среда ИАРОФ ФГБОУ ВО «КГТУ»: <http://eios.bgarf.ru/login/index.php>. Мультимедиа технологии, используемые для проведения занятий.

10.2 Интернет-ресурсы дисциплины

Интернет-ресурсы Интернет-ресурсы, применяемые при изучении дисциплины:

1. ЭБС «ИАРОФ» <http://bgarf.ru/academy/biblioteka/>
2. ЭБС «КГТУ» <http://www.kgtu.ru/library/>
3. Университетская библиотека Online (г.Москва) <https://bibliotekub.ru/>
4. Редакция базы данных POLPRED.COM <https://polpred.com/>
5. Научная лицензионная библиотека eLIBRARY.RU <https://elibrary.ru/defaultx.asp>
6. ЭБС "IPRbooks" <http://www.iprbookshop.ru/>
7. ЭБС "Лань" <https://e.lanbook.com/>
8. ЭБС ИЦ "Академия" <http://www.academia-moscow.ru/elibrary>

10.3 Программное обеспечение

Включают в себя обучающие программы определение оптимальных характеристик порция с использованием методов генетического алгоритма (Свидетельство о государственной регистрации программы для ЭВМ № 2015614020); Advanced ZIP Password Recovery (Open source)

11 Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины



Помещения для проведения лекционных занятий укомплектованы необходимой специализированной учебной мебелью и техническими средствами для представления учебной информации студентам, персональный компьютер преподавателя с мультимедиа-проектором и экраном. Программное обеспечение Microsoft Desktop Education (Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription. Антивирусное программное обеспечение: Kaspersky Total Space Security Russian.

Лабораторные работы проводятся в специализированных аудиториях: компьютерном классе № 248 в состав которого входят персональные ЭВМ, объединенные в локальную вычислительную сеть Ethernet, персональный компьютер преподавателя с мультимедиа-проектором и экраном; ауд.№ 440 в состав которой входят учебные стенды, персональный компьютер преподавателя с мультимедиа-проектором и экраном, стенды охранно-пожарной сигнализации. Плотная аудитория № 302.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Обеспечение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12 Фонд оценочных средств для проведения аттестации по дисциплине

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Основы информационной безопасности».

13 Особенности преподавания и освоения дисциплины

Под образовательными технологиями понимаются пути и способы формирования компетенций.

13.1 Пути и способы формирования компетенций.

В рамках дисциплины предусмотрены:

- лекции;

- лабораторные занятия: во время которых на занятиях наиболее полно используются возможности компьютерных информационных технологий, чтобы студенты приобретали практические навыки. При этом образовательные технологии направлены на усвоение теоретического и практического материала, на развитие интеллектуальных способностей студентов та-



		узловые вопросы курса. - при работе с электронными материалами необходимо обращаться по возможности к первоисточникам, а также указывать ссылки при копировании данных для их дальнейшего использования.	
4	Написание контрольной работы в виде реферативной формы	- при написании текста контрольной работы цитируемые фрагменты должны сопровождаться логическими авторскими ссылками, и содержать ссылки на источники копирования.	В зависимости от степени сложности письменной работы

14.2 Рекомендации по подготовке к лабораторным занятиям

Лабораторные занятия - форма организации учебного процесса, во время которой на занятиях наиболее полно используются возможности компьютерных информационных технологий, чтобы студенты приобретали навыки решения задач.

Основной целью лабораторного занятия является проверка глубины понимания студентом изучаемой темы, учебного материала и умения изложить его содержание ясным и четким языком, развитие самостоятельного мышления и творческой активности у студента. На лабораторных занятиях предполагается рассматривать наиболее важные, существенные, сложные вопросы которые, как свидетельствует преподавательская практика, наиболее трудно усваиваются студентами.

Уготовиться к лабораторным занятиям необходимо заблаговременно. Подготовка включает в себя следующее:

- изучить конспекты лекций, соответствующие разделы учебника, учебного пособия, содержание рекомендованных нормативных правовых актов;
- нужно изучить дополнительную литературу по теме занятия, делая при этом необходимые выписки, которые понадобятся при обсуждении на уроке;
- следует записывать возникшие во время самостоятельной работы с учебниками и научной литературы вопросы, чтобы затем получить на них ответы;
- следует обращаться за консультацией к преподавателю.

Изучение материала к лабораторному занятию следует начать с просмотра конспектов лекций. Восстановив в памяти материал, студент приводит в систему основные положения темы, вопросы темы, выделяя в ней главное и новое, на что обращалось внимание в лекции. Затем следует внимательно изучить соответствующую главу учебника. Для более углубленного изучения вопросов рекомендуется конспектирование основной и дополнительной литературы.

В общем виде рекомендации по подготовке к лабораторному занятию сводятся к следующему: студент должен постоянно проливать стремление к овладению предметом, используя при этом все имеющиеся ресурсы знаний. При этом образовательные технологии направлены на усвоение теоретического и практического материала, на развитие интеллектуальных способностей студентов таких, как умение анализировать ошибки, синтезировать и структурировать информацию, принимать решения, делать окончательные выводы.



ких, как умение анализировать ошибки, синтезировать и структурировать информацию, принимать решения, делать окончательные выводы.

- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к лабораторным занятиям, выполнение рефератов, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к такому же контролю усвоения, к экзамену;

- тестирование по отдельным темам дисциплины, по разделам программы;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы

Реализация программы предполагает использование интерактивных форм проведения занятий. Проведение лабораторных занятий подразумевает обучение, построенное на индивидуальной деятельности студентов, в том числе с использованием персонального компьютера.


14 Методические указания по освоению дисциплины

14.1 Рекомендации по планированию и организации времени, необходимого для изучения дисциплины

Для более глубокого усвоения студентом предмета, понимания основных проблем ИБ рекомендуется следующим образом организовать время, необходимое для изучения дисциплины (таблица 14.1).

Таблица 14.1 - План организации времени, необходимого для изучения дисциплины студентом

№	Вид деятельности	Рекомендации по организации деятельности	Продолжительность времени
1	Изучение конспекта лекции	- изучение конспекта рекомендуется проводить как минимум два раза: в тот же день после лекции и за день перед следующей лекцией; - при работе с лекцией необходимо отметить для себя имеющиеся вопросы, желательно письменные; - вести конспект рекомендуется аккуратно и регулярно.	от 15 до 30 минут
2	Подготовка к лабораторной работе	- обязательно знание лекционного материала; - выполнение заданий преподавателя, используя методические рекомендации и различные источники информации.	от 30 до 50 минут (при необходимости в несколько этапов)
3	Изучение материала по дополнительным источникам информации (учебники, спец. литература, публикации в научных журналах, интернет – источники)	- при работе с литературой следует вести записи основных положений (конспектировать отдельные разделы, выписывать новые термины и раскрывать их содержание); - необходимо проработать ряд литературных источников и, прежде всего учебные пособия, в которых наиболее полно отражены и систематизированы	В зависимости от поставленных задач

 БГАРФ	Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «Калининградский государственный технический университет»	стр. 2 из 19
	Рабочая программа дисциплины «Основы информационной безопасности»	
	Версия: 1	25.05.03 «Техническая эксплуатация транспортного радиооборудования» и специализации 25.05.03 «Инфокоммуникационные системы на транспорте и их информационная защита»

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« 07 » 06 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « 07 » 06 2018 г. № 9

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите

Визирование РПД для исполнения в очередном учебном году

Утверждаю: И.о. декана РТФ _____ В.А. Баженов

« ____ » _____ 20__ г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 20__-20__ учебном году на заседании кафедры Информационной безопасности

Протокол от « ____ » _____ 20__ г. № _____

Зав. кафедрой «Информационная безопасность» _____ к.ф.-м.н., доцент Н.Я. Великите