	Балтийская государственная академия рыбопромыслового флота		
	Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»		
Версия: 1	Дата выпуска версии: 15.05.18		стр. 1 из 20

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.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

(наименование дисциплины)

базовой части образовательной программы по специальности

10.05.03 «Информационная безопасность автоматизированных систем»

Специализация программы

Обеспечение информационной безопасности распределенных информационных систем

(наименование специализации программы)

Факультет – **РАДИОТЕХНИЧЕСКИЙ**

Кафедра – **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Калининград 2018

	Балтийская государственная академия рыбопромыслового флота		
	Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»		
	Версия: 1	Дата выпуска версии: 15.05.18	стр. 2 из 20

Визирование РПД для исполнения в очередном учебном году

УТВЕРЖДАЮ:

и.о. декана РТФ _____ В.А.Баженов

«27» июня 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018 – 2019 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «14» июня 2018 г. № 9

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

УТВЕРЖДАЮ:

и.о. декана РТФ_____ В.А.Баженов

«____» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019 – 2020 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «___» _____2019 г. №

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

1. Цель освоения дисциплины.

1.1. Цели дисциплины

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», содействует формированию мировоззрения и системного мышления.

Основная цель преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» - раскрыть:

−основы правового регулирования отношений в информационной сфере;

−конституционные гарантии прав граждан на получение информации и механизм их реализации;

−понятия и виды защищаемой информации по законодательству РФ;

−систему защиты государственной тайны;

−основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности;

−понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы.

1.2. **Задачи дисциплины – дать основы:**

– законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;

– понятий и видов защищаемой информации по законодательству РФ;

– правовых режимов конфиденциальной информации;

– правового режима защиты государственной тайны, системы защиты государственной тайны;

– лицензирования и сертификации в области защиты информации, в том числе государственной тайны;

– правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);

– защиты интеллектуальной собственности;

– правовой регламентации охранной деятельности;

– правового регулирования взаимоотношений администрации и персонала в области защиты информации;

– международного законодательства в области защиты информации;

– знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах проведения расследований.

– угроз информационной безопасности объекта;

– организации службы безопасности объекта;

– подбора и работы с кадрами в сфере информационной безопасности;

– организации и обеспечения режима конфиденциальности.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Компетенции выпускника ОП ВО и этапы их формирования в результате изучения дисциплины	Этапы формирования компетенции		Знания, умения и навыки, характеризующие этапы формирования компетенций
1			2
ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	**Знать:**		**Знать:** Основные проблемы в области информационной безопасности **Уметь** использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач **Владеть** основными методами научного познания
	Уровень 1	основные составляющие национальных интересов Российской Федерации в информационной сфере.	
	Уровень 2	сущность и понятие информационной безопасности, характеристику ее составляющих.	
	Уровень 3	цели, задачи, принципы и основные направления обеспечения информационной безопасности государства.	
	Уметь		
	Уровень 1	самостоятельно получать новые знания по предметной области и в областях, непосредственно примыкающих к объектам будущей профессиональной деятельности	
	Уровень 2	самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять границы использования знаний	
	Уровень 3	самостоятельно получать знания для решения исследовательских задач, задач повышенной сложности	
	Владеть		
	Уровень 1	технологиями систематизации и накопления научных знаний в предметной области	
	Уровень 2	методиками выполнения научно-исследовательских работ	
	Уровень 3	методологией прикладных научных исследований в предметной области	
ОК-6 - способность работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные, культурные и иные различия	**Знать:**		**Знать:** области управленческой деятельности; порядок выработки и реализации управленческих решений; содержание управленческой работы руководителя под-
	Уровень 1	требования к сотрудникам организации, допущенным к конфиденциальной информации	
	Уровень 2	основы правового регулирования взаимоотношений администра-	

		ции и персонала в области защиты информации, основные критерии приема на работу, связанную с сохранением тайны	разделения; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем **Уметь:** осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач **Владеть** навыками обоснования, выбора, реализации и контроля результатов управленческого решения
	Уровень 3	теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию, основы правового регулирования взаимоотношений администрации и персонала в области защиты информации	
	Уметь		
	Уровень 1	применять действующую законодательную базу в области информационной безопасности	
	Уровень 2	организовывать работу с персоналом, обладающим конфиденциальной информацией	
	Уровень 3	самостоятельно получать знания для решения исследовательских задач, задач повышенной сложности	
	Владеть		
	Уровень 1	технологиями систематизации и накопления научных знаний в предметной области	
	Уровень 2	методиками выполнения научно-исследовательских работ	
	Уровень 3	методологией прикладных научных исследований в предметной области	
ОПК-6 - способность применять нормативные правовые акты в профессиональной деятельности	**Знать**		**Знать:** правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; основные отечественные и зарубежные стандарты в области информационной безопасности; терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** применять действующую законодательную базу в области обеспечения информационной безопасности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	Уровень 1	понятие и виды защищаемой информации по законодательству РФ	
	Уровень 2	правовые основы защиты информации с использованием технических средств	
	Уровень 3	законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации	
	Уметь		
	Уровень 1	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	
	Уровень 2	применять действующую законодательную базу в области информационной безопасности	
	Уровень 3	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов, анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития	

	Владеть		**Владеть:** навыками работы с нормативными правовыми актами; навыками работы с технической документацией на ЭВМ и вычислительные системы; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках
	Уровень 1	навыками разработки и использования нормативно-методическими материалами по регламентации системы организационной защиты информации	
	Уровень 2	методиками выполнения научно-исследовательских работ	
	Уровень 3	методологией прикладных научных исследований в предметной области	
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	**Знать**		**Знать:** основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня (объектно-ориентированное программирование); **Уметь:** применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации **Владеть:** навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках
	Уровень 1	классификацию и характеристики информационных баз и хранилищ	
	Уровень 2	информационные базы и хранилища, порядок обращения к ним и поиска информации	
	Уровень 3	порядок обработки патентной информации, информации по интеллектуальной собственности	
	Уметь		
	Уровень 1	определить пути получения научно-технической информации, обобщать и систематизировать информацию	
	Уровень 2	использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины	
	Уровень 3	проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию	
	Владеть		
	Уровень 1	навыками систематизации, обобщения справочной, нормативно-технической информации	
	Уровень 2	навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов	
	Уровень 3	навыками обобщения и систематизации научно-технической информации из предметной области исследований и других областей науки и техники, непосредственно примыкающих к проведенным исследованиям	

ПК-11 - способность разрабатывать политику информационной безопасности автоматизированной системы	**Знать**		**Знать:** основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня (объектно-ориентированное программирование); **Уметь:** применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации **Владеть:** навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках
	Уровень 1	уровни политики безопасности и ответственные за них, методы оценки рисков	
	Уровень 2	теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию	
	Уровень 3	методы анализа и оценки угроз ИБ объектов информатизации, средства и методы физической защиты объектов, принципы построения систем защиты информации автоматизированных систем	
	Уметь		
	Уровень 1	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	
	Уровень 2	анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития	
	Уровень 3	выявлять уязвимости автоматизированных систем и ее системы защиты, определять необходимые и достаточные затрат на информационную безопасность предприятия	
	Владеть		
	Уровень 1	методами формирования требований по защите информации	
	Уровень 2	методиками выполнения научно-исследовательских работ	
	Уровень 3	методологией прикладных научных исследований в предметной области	
ПК-20 - способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать**		**Знать:** программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях. **Уметь:** проводить выбор программно-аппаратных средств обеспечения информационной безопасности для ис-
	Уровень 1	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	
	Уровень 2	современные подходы к построению систем защиты информации в автоматизированных системах	
	Уровень 3	нормативную базу эксплуатации и эксплуатационную документацию автоматизированных систем	
	Уметь		

	Уровень 1	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	пользования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы **Владеть:** навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками работы с нормативными правовыми актами; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ
	Уровень 2	применять действующую законодательную базу в области информационной безопасности	
	Уровень 3	выбирать и анализировать эксплуатационные показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
	Владеть		
	Уровень 1	навыками разработки нормативно-методических материалов по регламентации системы организационной защиты информации	
	Уровень 2	навыками работы с нормативно-правовыми актами	
	Уровень 3	методологией прикладных научных исследований в предметной области	
ПК-21 - способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Знать:**		**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем **Владеть:** навыками, эксплуатации и администрировани (в части, касающейся разграничения доступа, аутентифи кации и аудита) баз данных, локальных компьютерны сетей, программных систем с учетом требований по обес печению информационной безопасности
	Уровень 1	направления создания правовой базы в области информационной безопасности	
	Уровень 2	причины нарушения целостности информации	
	Уровень 3	особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну	
	Уметь		
	Уровень 1	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	
	Уровень 2	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	
	Уровень 3	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	
	Владеть		
	Уровень 1	технологиями систематизации и накопления научных знаний в предметной области	
	Уровень 2	методиками выполнения научно-исследовательских работ	

	Уровень 3	методологией прикладных научных исследований в предметной области	
ПК-22 - способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знать**		**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем **Владеть:** навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
	Уровень 1	основные принципы, реализуемые при разработке политики информационной безопасности организации	
	Уровень 2	основные виды политики информационной безопасности организации	
	Уровень 3	основные этапы разработки концепции безопасности организации, содержание документов политики информационной безопасности	
	Уметь		
	Уровень 1	разрабатывать функциональные обязанности должностных лиц организации по вопросам защиты информации	
	Уровень 2	вносить необходимые изменения и дополнения в организационно-распорядительные документы по вопросам обеспечения информационной безопасности программно-информационных ресурсов автоматизированных систем	
	Уровень 3	производить периодический анализ состояния и контроль эффективности реализуемых мер защиты информации	
	Владеть		
	Уровень 1	навыками соблюдения правил защиты информации	
	Уровень 2	навыками разработки концепции информационной безопасности организации (предприятия)	
	Уровень 3	методикой управления инцидентами и мониторингом подсистемы информационной безопасности АС	
ПК-23 - способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**Знать**		**Знать:** основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры **Уметь:** определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем
	Уровень 1	основные меры обеспечения информационной безопасности АС	
	Уровень 2	основные мероприятия по защите информации от утечки по техническим каналам	
	Уровень 3	основные мероприятия по пресечению несанкционированного доступа к конфиденциальной информации	
	Уметь		
	Уровень 1	разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС организации	

	Уровень 2	обеспечивать соблюдение соответствующего режима ограничения и разграничения доступа к информации, контроль выполнения установленных правил работы в АС	**Владеть:** навыками обоснования, выбора, реализации и контроля результатов управленческого решения; навыками организации и обеспечения режима секретности; навыками работы с технической документацией на ЭВМ и вычислительные системы
	Уровень 3	производить обобщенное описание объектов защиты, используя основные правила построения модели угроз и модели нарушителя, с дальнейшей реализацией принципов контроля эффективности системы информационной безопасности АС	
	Владеть		
	Уровень 1	навыками разработки концепции информационной безопасности организации (предприятия)	
	Уровень 2	методикой управления инцидентами и мониторингом подсистемы информационной безопасности АС	
	Уровень 3	навыками соблюдения правил защиты информации	

3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.29 «Организационное и правовое обеспечение информационной безопасности» относится к числу дисциплин базовой части.
Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:
«Правоведение» - основными правовыми понятиями;
«Основы информационной безопасности» - основными понятиями и терминологией в области обеспечения информационной безопасности.
Дисциплина необходима для освоения производственной практики. В свою очередь, данная дисциплина является обеспечивающей для написания выпускной квалификационной работы.

4. Содержание дисциплины

Индекс, наименование дисциплины	Содержание дисциплины (дидактические единицы)	Всего часов
Б1.Б.29	Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; государственная тайна как особый вид защищаемой информации; конфиденциальная информация; система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации; лицензирование и сертификация в области защиты информации, в том числе государственной тайны; правовые основы защиты информации с использованием технических средств; защита интеллектуальной собственности; международное законодательство в области защиты информации; преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации. Анализ и оценка угроз информационной безопасности объекта; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; обеспечение информационной безопасности объекта при осуществлении международного научно-технического и экономического сотрудничества.	180

РАЗДЕЛ 1. Законодательство РФ в области информационной безопасности.
Тема 1.1. Структура и основные направления развития законодательной базы в области информационной безопасности.
Тема 1.2. Основные руководящие документы в области информационной безопасности.
РАЗДЕЛ 2. Правовые основы защиты государственной тайны.
Тема 2.1. Правовой режим защиты государственной тайны.
Тема 2.2. Организация защиты государственной тайны при обмене информации.
РАЗДЕЛ 3. Правовые основы защиты конфиденциальной информации.
Тема 3.1. Защита права на личную информацию с ограниченным доступом.
Тема 3.2. Основные положения по организации защиты коммерческой тайны предприятия.
РАЗДЕЛ 4. Правовое регулирование деятельности организаций в области информационной безопасности.
Тема 4.1. Система лицензирования в информационной сфере.
Тема 4.2. Система сертификации в информационной сфере.
Тема 4.3. Система аттестации объектов обработки конфиденциальной информации.
РАЗДЕЛ 5. Юридическая ответственность за правонарушения в области информационной безопасности.
Тема 5.1. Понятия и виды юридической ответственности за нарушение правовых норм по защите информации.

Тема 5.2. Компьютерные преступления и правовая защита от них.
РАЗДЕЛ 6. Концептуальные положения организационного обеспечения информационной безопасности.
Тема 6.1. Задачи организационного обеспечения информационной безопасности.
Тема 6.2. Угрозы информационной безопасности на объекте.
РАЗДЕЛ 7. Организационная структура системы обеспечения информационной безопасности.
Тема 7.1. Организация службы безопасности объекта.
Тема 7.2. Организация внутриобъектового режима.
Тема 7.3. Подбор сотрудников и работа с кадрами.
РАЗДЕЛ 8. Организация и обеспечение режима секретности на объекте.
Тема 8.1. Организация и обеспечение секретного делопроизводства.
Тема 8.2. Обеспечение режима секретности при деятельности объекта.
РАЗДЕЛ 9. Охрана объектов.
Тема 9.1. Средства и методы физической защиты объектов.
Тема 9.2. Организация охраны объекта.
Тема 9.3. Организация пропускного режима.

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней

Таблица 2 - Структура дисциплины по очной форме обучения

Номер и наименование раздела, темы	Объем учебной работы (час.)					
	Лекции	ЛЗ	ПЗ	СР	Контроль	Всего
Семестр – 5 (5 ЗЕТ, 180 час.)						
РАЗДЕЛ 1. Законодательство РФ в области информационной безопасности.	**4**	**4**	**-**	**9**	**2**	**19**
Тема 1.1. Структура и основные направления развития законодательной базы в области информационной безопасности.	2	-	-	-	-	2
Тема 1.2. Основные руководящие документы в области информационной безопасности.	2	4	-	9	-	15
РАЗДЕЛ 2. Правовые основы защиты государственной тайны.	**4**	**-**	**2**	**9**	**2**	**17**
Тема 2.1. Правовой режим защиты государственной тайны.	2	-	-	-	-	2
Тема 2.2. Организация защиты государственной тайны при обмене информации.	2	-	2	9	-	13
РАЗДЕЛ 3. Правовые основы защиты конфиденциальной информации.	**4**	**-**	**2**	**9**	**2**	**17**
Тема 3.1. Защита права на личную информацию с ограниченным доступом.	2	-	-	9	-	11
Тема 3.2. Основные положения по организации защиты коммерческой тайны предприятия.	2	-	2	-	-	4
РАЗДЕЛ 4. Правовое регулирование деятельности организаций в области информационной безопасности.	**4**	**6**	**2**	**9**	**2**	**23**
Тема 4.1. Система лицензирования в информационной сфере.	1	2	1	3	-	7

Тема 4.2. Система сертификации в информационной сфере.	1	2	1	3	-	7
Тема 4.3. Система аттестации объектов обработки конфиденциальной информации.	2	2	-	3	-	7
РАЗДЕЛ 5. Юридическая ответственность за правонарушения в области информационной безопасности.	**4**	**-**	**4**	**9**	**2**	**19**
Тема 5.1. Понятия и виды юридической ответственности за нарушение правовых норм по защите информации.	2	-	-	-	-	2
Тема 5.2. Компьютерные преступления и правовая защита от них.	2	-	4	9	-	15
РАЗДЕЛ 6. Концептуальные положения организационного обеспечения информационной безопасности.	**4**	**2**	**2**	**9**	**2**	**19**
Тема 6.1. Задачи организационного обеспечения информационной безопасности.	2	2	2	9	-	15
Тема 6.2. Угрозы информационной безопасности на объекте.	2	-	-	-	-	2
РАЗДЕЛ 7. Организационная структура системы обеспечения информационной безопасности.	**4**	**6**	**2**	**9**	**2**	**23**
Тема 7.1. Организация службы безопасности объекта.	1	2	2	3	-	8
Тема 7.2. Организация внутриобъектового режима.	1	2	-	3	-	6
Тема 7.3. Подбор сотрудников и работа с кадрами.	2	2	-	3	-	7
РАЗДЕЛ 8. Организация и обеспечение режима секретности на объекте.	**4**	**-**	**2**	**9**	**2**	**17**
Тема 8.1. Организация и обеспечение секретного делопроизводства.	2	-	2	-	-	4
Тема 8.2. Обеспечение режима секретности при деятельности объекта.	2	-	-	9	-	11
РАЗДЕЛ 9. Охрана объектов.	**4**	**-**	**2**	**9**	**2**	**17**
Тема 9.1. Средства и методы физической защиты объектов.	2	-	2	3	-	7
Тема 9.2. Организация охраны объекта.	1	-	-	3	-	4
Тема 9.3. Организация пропускного режима.	1	-	-	3	-	4
Всего	36	18	18	**81**	**18**	**171**
Подготовка к сдаче экзамена	**-**	**-**	**-**	**-**	**9**	**9**
Итого по дисциплине	**36**	**18**	**18**	**81**	**27**	**180**
	72					

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СР – самостоятельная работа студента

6. Лабораторные занятия (работы)

Таблица 3 - Лабораторные занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ЛЗ	Количество часов ЛЗ
Семестр – 5 (18 час.)			
1.	6.1.	Закрепление права предприятия на защиту информации в нормативных документах	2
2.	4.1.; 4.2.	Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации	4
3.	4.3.	Аттестация помещений по требованиям безопасности информации	4
4.	1.2.	Правовые нормы защиты информации в автоматизированных системах	2
5.	7.1.; 7.2.	Создание системы информационной безопасности предприятия	4
6.	7.3.	Обеспечение защиты информации при работе с кадрами	2
Всего за семестр:			18
Итого по дисциплине			**18**

7. Практические занятия

Таблица 3 – Практические занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ПЗ	Количество часов ЛЗ
Семестр – 5 (18 час.)			
1.	2.2.	Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны.	2
2.	4.1.; 4.2.	Изучение порядка осуществления лицензирования и сертификации в области защиты информации.	2
3.	3.2.	Изучение вопросов защиты интеллектуальной собственности в Российской Федерации.	2
4.	5.2.	Состав компьютерных преступлений. Нормы ответственности за правонарушения в информационной сфере.	4
5.	7.1.	Правовые основы использования организационных средств защиты информации.	2
6.	6.1.	Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.	2
7.	8.1.	Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных.	2
8.	9.1	Правовое регулирование защиты информации с использованием технических средств и противодействия угрозам информационной безопасности.	2
Всего за семестр:			18
Итого по дисциплине			**18**

8. Самостоятельная работа студента

Таблица 4 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СР	Количество часов СР	Форма контроля, аттестации
Семестр – 4			
1.	Государственная тайна как особый вид защищаемой информации и ее характерные признаки.	9	конспект лекций, реферат
2.	Правовая регламентация лицензионной и сертификационной деятельности в области ИБ.	9	конспект лекций
3.	Модели нарушителей.	9	конспект лекций
4.	Особенности инструментального контроля эффективности инженерно-технической защиты информации.	9	конспект лекций
5.	Механизмы контроля физического доступа	9	конспект лекций, реферат
6.	Принципы организации службы информационной безопасности	9	конспект лекций
7.	ФЗ «О персональных данных»	9	конспект лекций
8.	ФЗ «О правовой охране программ для ЭВМ и баз данных»	9	конспект лекций
9.	Правовая защита информации в сфере высоких технологий	9	конспект лекций
Всего за семестр:		**81**	
Итого по дисциплине		**81**	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

9.1. Основная учебная литература

1. Ищейнов, В. Я. Защита конфиденциальной информации : учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – М. : ФОРУМ, 2013. – 256 с. (наличие в библиотеке БГАРФ - 15 экз.)

2. Кузнецов, А. В. Основы защиты информации : учеб. пособие / В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с. (наличие в библиотеке БГАРФ - 110 экз.)

9.2. Дополнительная учебная литература

1. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / А. А. Стрельцов [и др.] ; под общ. ред. А. А. Стрельцова. – М. : Академия, 2008. – 256 с. (наличие в библиотеке БГАРФ - 12 экз.)

2. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. - СПб. : Питер, 2008. - 272 с. (наличие в библиотеке БГАРФ - 15 экз.)

3. Просис, Крис. Расследование компьютерных преступлений / К. Просис, К. Мандиа ; пер. О. Труфанов. – М. : ЛОРИ, 2013. – 76 с. (наличие в библиотеке БГАРФ - 20 экз.)

9.3. Периодические издания

1. Лачихина, А. Б. Подходы и методы управления информационной безопасностью в процессе управления промышленным предприятием / А. Б. Лачихина, А. А. Петраков. // Вопросы радиоэлектроники. – 2017. – №11. – С.48-51.

2. Домуховский, Н. А. Обзор закона "О безопасности критической информационной инфраструктуры Российской Федерации" / Н. А. Домуховский. // Защита информации. Инсайд. – 2017. – №6. – С.8-13.

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Ресурсы информационно-телекоммуникационной сети «Интернет»:

– «Консультант Плюс» (www.consultant.ru);
– «Гарант» (www.garant.ru);
– http://www.rg.ru/dok/ [On-line] – опубликованные нормативные-правовые акты РФ;
– http://fstec.ru;
– http://www.confident.ru;
– http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/;
– http://www.iqlib.ru - электронная интернет библиотека;
– http://www.biblioclub.ru - полнотекстовая электронная библиотека;
– http://www.elibrary.ru - научная электронная библиотека.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем: программное обеспечение Microsoft Desktop Education.

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

Используется лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.1.2. Материально-техническое обеспечение для лабораторных, практических занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 440.

Состав оборудования: столы учебные – 10 шт., стол преподавательский – 1 шт., стулья учебные – 20 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды охранно-пожарной сигнализации – 3 шт.

Стенды со специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок и контроля эффективности защиты (подавитель микрофонов «Шаман», детектор поля ST 007, портативный измеритель частоты и мощности MPF-8000).

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютер MUSTIFF (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением: Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

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

Освоение 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 «Организационное и правовое обеспечение информационной безопасности».

13. Особенности преподавания и освоения дисциплины

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешени-

ем их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы. Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

Перед началом занятий преподаватель проводит инструктаж по технике электробезопасности и пожарной безопасности. Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих контролей, а также итоговой аттестации в форме экзамена по итогам учебного семестра.

Текущие контроли предназначены для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Они могут осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины. Текущие контроли предполагают постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением оценок в журнале учета успеваемости.

К экзамену допускаются студенты, имеющие по всем текущим контролям положительные оценки.

14. Методические указания по освоению дисциплины

Планирование и организация времени, необходимого на изучение дисциплины, предусматривается ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и рабочим учебным планом подготовки специалистов. Объем часов и формы работы по изучению дисциплины распределены в рабочей программе соответствующей дисциплины.

14.1 Общие сведения о дисциплине

Цель дисциплины «Организационное и правовое обеспечение информационной безопасности» — заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

14.2. Виды занятий и способы контроля

В соответствии с рабочим учебным планом дисциплина «Организационное и правовое обеспечение информационной безопасности» включает следующие виды занятий: лекции, лабораторные занятия, практические занятия, самостоятельная работа студентов.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины, которые находят выражение в агрегированности и комбинации подходов. В подборе материала к занятиям следует руководствоваться рабочей программой

учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в аудитории и нацелить их на проведение самостоятельной работы с учетом количества часов, отведенных на нее учебным планом. Рекомендуя литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе ее электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

В конце лекции необходимо делать выводы и ставить задачи на самостоятельную работу. Лабораторные и практические занятия направлены на закрепление лекционного материала. При подготовке к лабораторным занятиям руководствоваться «Методическими указаниями по выполнению лабораторных работ по дисциплине «Организационное и правовое обеспечение информационной безопасности» и «Методическими указаниями по выполнению практических работ по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Самостоятельная работа студентов заключается в подготовке к практическим и лекционным занятиям и выполнении домашних заданий, выдаваемых преподавателем по каждому из разделов дисциплины. В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

При самостоятельной проработке курса обучающиеся должны: просматривать основные определения и факты; повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы; изучить рекомендованную основную и дополнительную литературу; самостоятельно выполнять задания для самостоятельной подготовки; использовать для самопроверки материалы фонда оценочных средств.

При самостоятельной работе руководствоваться «Методические указания по организации и контролю самостоятельной работы студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности».

	Балтийская государственная академия рыбопромыслового флота		
	Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» по специальности 10.05.03 «Информационная безопасность автоматизированных систем»		
	Версия: 1	Дата выпуска версии: 15.05.18	стр. 20 из 20

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы – доцент кафедры «Информационная безопасность» Жестовский А.Г.

Программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность» (протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой «Информационная безопасность» _____/Великите Н.Я./

Программа рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета (протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____/Жестовский А.Г./