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

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

(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

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 «Разработка и эксплуатация защищенных автоматизированных систем» обеспечивает формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации.

1.2. Задачи дисциплины:

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем;
- формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.
- определение места системы защиты информации в корпоративной информационной системе;
- определение и классификация методов защиты информации в распределенной вычислительной сети предприятия;
- раскрытие принципов, методов и технологии проектирования систем защиты информации для корпоративных информационных систем;
- изучение научных, прикладных и методологических аспектов организации технологии защиты автоматизированных систем;
- изучение научных и прикладных аспектов организации защищенной инфраструктуры корпоративной информационной системы;
- закрепление полученных знаний с целью их применения на практике после окончания учебы;
- управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного доступа к ее информационным, программным и аппаратным ресурсам;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;
- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

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
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-3: способность проводить анализ защищенности автоматизированных систем	**Знать**		**Знать:** требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных компьютерных сетях; технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации **Уметь:** применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; **Владеть:** навыками организации и обеспечения режима секретности
	Уровень 1	классификацию АС и перечень требований по защите информации к каждому классу автоматизированных систем	
	Уровень 2	требования стандарта ISO по номенклатуре услуг, предоставляемых системой безопасности	
	Уровень 3	основные положения концепции защиты и показатели защищенности АС от несанкционированного доступа к информации	
	Уметь		
	Уровень 1	определять цель, объект и место проведения анализа АС, уточнять вид проводимого инструментального контроля, составлять перечень исследуемых систем	
	Уровень 2	применять существующую методическую базу проведения оценки защищенности технических средств от утечки информации	
	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-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**Знать**		**Знать:** классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя; определение базовой модели нарушителя; неформальной модели нарушителя; типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах; определение категории нарушителя; типологию нарушителей по характеру поведения **Уметь:** устанавливать приоритеты целей безопасности для субъекта отношений; определять перечень актуальных источников угроз; определять перечень актуальных уязвимостей; оценивать взаимосвязь угроз,
	Уровень 1	основные этапы проведения анализа уязвимости объекта, при разработке модели угрозы и модели нарушителя	
	Уровень 2	основные виды моделей воздействия нарушителей информационной безопасности АС	
	Уровень 3	основные модели и методики оценки показателей уязвимости (устойчивости), реализуемые при создании эффективной системы безопасности	
	Уметь		
	Уровень 1	классифицировать возможные виды ущерба от нарушения безопасности информации в АС	
	Уровень 2	оценивать влияние угроз информационной безопасности АС на тактико-технические характеристики аппаратных средств обработки информации	

	Уровень 3	производить оценку снижения эффективности процесса обработки информации, вызванного ухудшением ТХ аппаратных средств, качества программных средств, исходной и обрабатываемой информации в АС	источников угроз и уязвимостей; определять перечень возможных атак на объект; описывать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей. **Владеть:** навыками установки приоритетов целей безопасности для субъекта отношений; определения перечня возможных атак на объект; описать возможные последствия реализации угроз.
	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-5: способность проводить анализ рисков информационной безопасности автоматизированной системы	**Знать**		**Знать:** методологию оценку риска; оценку ущерба от реализацию угроз; выбор мер и средств защиты в соответствии с уровнем риска; внедрение и тестирование средств защиты; показатели предотвращенного ущерба; методики оценки угроз **Уметь:** выбирать методику оценки угроз; производить оценку ущерба от угроз безопасности информации; производить оценки потенциально возможных угроз информационной системы и средств защиты **Владеть:** методикой идентификации и оценки угроз; методикой оценки риска; методикой определения вероятности угроз; методикой оценки ущерба в зависимости от применяемы средств защиты
	Уровень 1	структуру профиля защиты АС и исходные данные для его разработки	
	Уровень 2	основные методы оценки эффективности построения систем информационной безопасности	
	Уровень 3	структуру автоматизированных систем и принципы ее функционирования, основные проблемы защиты информационно-технологических ресурсов организации	
	Уметь		
	Уровень 1	применять средства, обеспечивающие разграничение доступа к информации в защищенных АС	
	Уровень 2	применять средства, обеспечивающие защиту информации при передаче ее по каналам связи	
	Уровень 3	применять средства, обеспечивающие защиту от воздействия программ-вирусов	
	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-6: способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Знать**		**Знать: с**пособы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информа-
	Уровень 1	порядок разработки, внедрения и эксплуатации автоматизированных систем, отвечающих требованиям информационной безопасности	
	Уровень 2	организацию обеспечения информационной безопасности при	

		эксплуатации защищенных АС	ции.
	Уровень 3	основные средства анализа защищенности автоматизированных систем	**Уметь: о**пределять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации
	Уметь		
	Уровень 1	производить анализ и оценку защищенности автоматизированных систем	
	Уровень 2	проводить оценку функциональной целостности организационно-технической системы безопасности АС	
	Уровень 3	применять типовые модели анализа проектных решений по обеспечению безопасности АС	
	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	**Владеть: м**етодикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-13: способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать**		**Знать:** методы проектирования средств защиты информации
	Уровень 1	принципы и правила построения защищенных автоматизированных систем предприятия (организации)	**Уметь:** разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средств защиты информации
	Уровень 2	формальные модели безопасности и основные принципы построения модели защиты АС	
	Уровень 3	основные принципы и методы планирования функционирования защищенных автоматизированных систем	**Владеть:** методами исследования информационно-технологических ресурсов, методами проектирования средств защиты информации
	Уметь		
	Уровень 1	производить управление доступом к устройствам и отчуждаемым накопителям защищенной АС	
	Уровень 2	разрабатывать требования к виртуальным системам защиты информационного потока автоматизированной системы предприятия (организации)	
	Уровень 3	разрабатывать технические задания на создание подсистем информационной безопасности защищенных автоматизированных систем	

	Владеть		
	Уровень 1	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных систем	
	Уровень 2	навыками работы с нормативно-правовыми актами	
	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**		
	Уровень 1	автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	**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 использования 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	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	
	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-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:**
	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		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	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-24: способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**Знать**		**Знать:** автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; меры (компоненты) обеспечения безопасности компьютерных систем **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 **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 1	основные способы оптимизации процедуры оценки соответствия требованиям защищенности автоматизированных систем	
	Уровень 2	порядок создания продуктов и систем информационных технологий, удовлетворяющих требованиям информационной безопасности	
	Уровень 3	порядок разработки профиля защиты и задания по информационной безопасности, защищенных АС	
	Уметь		
	Уровень 1	исследовать эффективность создаваемых защищенных средств автоматизации	
	Уровень 2	проводить технико-экономическое обоснование применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
	Уровень 3	реализовывать планы обеспечения бесперебойной работы организации для случаев вирусного заражения и планы резервного копирования всех необходимых данных и программ и их восстановления	
	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-25: способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	**Знать**		**Знать:** основные методы восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций **Уметь:** восстанавливать работоспособность систем защиты информации при возникновении нештатных ситуаций **Владеть:** навыками организации восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций
	Уровень 1	организационные основы эксплуатации защищенных АС	
	Уровень 2	порядок обеспечения бесперебойной работы систем защиты информации в АС при возникновении нештатных ситуаций	
	Уровень 3	основной порядок предотвращения и восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций	
	Уметь		
	Уровень 1	планировать подготовку персонала организации (предприятия) при возникновении нештатных ситуаций	
	Уровень 2	принимать соответствующие меры по обнаружению внедрения вредоносного программного обеспечения АС и ликвидации последствий его атак	
	Уровень 3	реализовывать планы обеспечения бесперебойной работы организации для случаев вирусного заражения и планы резервного копирования всех необходимых данных и программ и их восстановления	
	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-26: способность администрировать подсистему информационной безопасности автоматизированной системы	**Знать**		**Знать:** действующую законодательную базу в области обеспечения информационной безопасности **Уметь:** разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации **Владеть:** навыками написания научно-технической документации, разработки нормативно-методической документации
	Уровень 1	принципы работы средств обеспечения безопасности	
	Уровень 2	принципы построения и функционирования сетей и протоколов стека TCP/IP	
	Уровень 3	работу сетей. IP адресация, модели ISO OSI, TCP	
	Уметь		
	Уровень 1	производить поиск уязвимостей с помощью специализированного ПО и их устранение	
	Уровень 2	настраивать систему защиты от НСД на базе Windows	
	Уровень 3	настраивать антивирусные системы	

	Владеть		
	Уровень 1	навыками поддержки работоспособности, администрирования и обеспечения бесперебойной работы специальных средств защиты информации	
	Уровень 2	навыками проведения аудитов, подготовки организационно-распорядительной документации и отчетов по ИБ	
	Уровень 3	навыками мониторинга и контроля функционирования средств обеспечения ИБ	
ПК-28: способность управлять информационной безопасностью автоматизированной системы	**Знать**		**Знать:** способы и механизмы управления информационной безопасностью автоматизированной системы **Уметь:** применять способы и механизмы управления информационной безопасностью автоматизированной системы **Владеть**: способами, механизмами способы и механизмы управления информационной безопасностью автоматизированной системы
	Уровень 1	нормативные и методические материалы по обеспечению защиты информации и соблюдению государственной тайны и конфиденциальной информации	
	Уровень 2	методы и процедуры выявления угроз безопасности информации на объектах информатизации организации	
	Уровень 3	порядок, методы и средства выявления угроз безопасности информации в ключевых системах информационной инфраструктуры	
	Уметь		
	Уровень 1	участвовать в разработке новых средств автоматизации контроля, схем аппаратуры контроля, моделей и систем защиты информации	
	Уровень 2	устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации	
	Уровень 3	разрабатывать предложения по совершенствованию и повышению эффективности средств информационной безопасности	
	Владеть		
	Уровень 1	навыками администрирования различных операционных систем, настройки и поддержки антивирусного ПО	
	Уровень 2	навыками выявления угроз безопасности информации, в том числе персональных данных, в информационных системах	
	Уровень 3	навыками проведения сравнительного анализа характеристик (показателей) разных классов средств обеспечению безопасности информации	
ПСК-7.3: способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	**Знать**		**Знать:** методы и технологии проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизи-
	Уровень 1	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации в сетях ЭВМ	
	Уровень 2	способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	

	Уровень 3	принципы построения систем защиты информации	рованных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации в автоматизированных и телекоммуникационных системах; принципы построения и функционирования систем и сетей передачи информации **Уметь:** выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и автоматизированных систем; применять стандартные методы и модели при решении типовых задач; проектировать и реализовывать политику безопасности компьютерной сети **Владеть навыками**: разработки модели угроз безопасности информации и нарушителей в автоматизированных системах; исследования программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; анализа информационной инфраструктуры и безопасности информации автоматизированных систем; разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем
	Уметь		
	Уровень 1	классифицировать и оценивать угрозы безопасности информации для объекта информатизации	
	Уровень 2	разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	
	Уровень 3	разрабатывать политики безопасности информации автоматизированных систем	
	Владеть		
	Уровень 1	навыками обоснования и контроля результатов управленческих решений в области безопасности информации автоматизированных систем	
	Уровень 2	навыками оценки информационных рисков	
	Уровень 3	навыками обоснования критериев эффективности функционирования защищенных автоматизированных систем	

3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.31 «Разработка и эксплуатация защищенных автоматизированных систем» относится к числу дисциплин базовой части.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Безопасность операционных систем» – знать критерии оценки эффективности и надежности средств защиты ОС, уметь использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем, владеть навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

«Безопасность сетей ЭВМ» – знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ, уметь эффективно использовать различные методы и средства защиты информации для компьютерных сетей, проводить мо-

ниторинг угроз безопасности компьютерных сетей, владеть навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;

«Основы информационной безопасности» – знать источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, владеть профессиональной терминологией в области информационной безопасности;

«Безопасность систем баз данных» – знать средства обеспечения безопасности данных, последовательность и содержание этапов проектирования баз данных, разрабатывать и администрировать базы данных, уметь применять средства обеспечения безопасности данных, реализовывать политику безопасности баз данных, навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;

«Электроника и схемотехника» – знать типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, уметь использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации, владеть навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры;

«Технологии и методы программирования» – знать современные технологии и методы программирования, методологии и методы проектирования программного обеспечения, принципы организации документирования разработки, процесса сопровождения программного обеспечения, уметь формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения, планировать разработку сложного программного обеспечения, проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.

«Комплексное обеспечение информационной безопасности автоматизированных систем» - знать основу комплексного подхода к решению задач информационной безопасности и правильно проводить комплексный анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, изучить методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, аттестация средств.

«Программно-аппаратные средства обеспечения информационной безопасности» - знать основные принципы построения систем защиты информации в операционных системах, вычислительных сетях и системах управления базами данных.

Дисциплина необходима для освоения преддипломной 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.31	Виды автоматизированных систем (АС). Общая характеристика систем автоматизации управленческой деятельности. Структура автоматизированных систем по видам обеспечения. Безопасность информации в автоматизированных системах. Классификационные схемы объектов защиты в автоматизированных (компьютерных) системах. Объекты защиты в защищенных автоматизированных системах. Общая характеристика стандартов безопасности компьютерных систем. Жизненный цикл защищенных автоматизированных систем – создание, эксплуатация и развитие, вывод из эксплуатации. Общие положения по эксплуатации изделий, комплексов, средств деятельности. Понятие эксплуатации и системы эксплуатации изделий. Организационные мероприятия по эксплуатации, их содержание и общая характеристика. Технические мероприятия по эксплуатации защищенных автоматизированных систем - применение по назначению, техническое обслуживание, ремонт, хранение, сбережение, транспортирование, консервация. Понятие, содержание и виды технического обслуживания (регламентных работ). Составляющие эксплуатации защищенных автоматизированных систем. Особенности эксплуатации защищенных автоматизированных систем. Угрозы безопасности на стадии эксплуатации и сопровождения АС. Органы системы управления эксплуатацией защищенных автоматизированных систем, функции и компетенции инженерно-технических, информационно-технологических и обеспечивающих подразделений, подразделений по защите информации. Планирование эксплуатации защищенных автоматизированных систем. Мониторинг, контроль, аудит безопасности в защищенных автоматизированных системах. Конструкторские эксплуатационные документы. Эксплуатационные документы организации – организационно-распорядительная документация (положения, инструкции, приказы) и учетно-отчетная документации по вопросам эксплуатации.	180

РАЗДЕЛ 1. РАЗРАБОТКА ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Тема 1.Защищенные АС. Основные понятия и классификация

1.1. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. 1.2. Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.

Тема 2. Основы организации разработки защищенных АС

2.1. Последовательность и содержание этапов разработки АС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. 2.2. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС.

Тема 3. Общие принципы проектирования защищенных АС

3.1. Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. 3.2. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Технологии создания отказоустойчивых систем.

РАЗДЕЛ 2. ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Тема 4. Основы эксплуатации защищенных АС

4.1. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Порядок обеспечения защиты информации при эксплуатации АС. 4.2. Технические и программные средства защиты АС от несанкционированного доступа. Организация технического обслуживания защищенных АС. Содержание и порядок ведения эксплуатационной документации. Методы проверки защищенных АС. Содержание и порядок ведения эксплуатационной документации.

Тема 5. Диагностика программных и аппаратных средств АС

5.1. Средства диагностирования защищенных АС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АС. Технологическое оборудование для ремонта аппаратных средств АС. 5.2. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования. Аппаратно-программные средства диагностики АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков. Диагностика программных и аппаратных средств АС

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 – А (5 ЗЕТ, 180 час.)						
Раздел 1. Разработка защищенных автоматизированных систем	**30**	**-**	**30**	**28**	**12**	**100**
Тема 1.Защищенные АС. Основные понятия и классификация	6	-	6	8	4	24
Тема 2. Основы организации разработки защищенных АС	12	-	12	10	4	38
Тема 3. Общие принципы проектирования защищенных АС	12	-	12	10	4	38
Раздел 2. Эксплуатация защищенных автоматизированных систем	**18**	**-**	**18**	**20**	**8**	**64**
Тема 4. Основы эксплуатации защищенных АС	12	-	12	10	4	38
Тема 5. Диагностика программных и аппаратных средств АС	6	-	6	10	4	26
Всего	**48**	**-**	**48**	**48**	**20**	**164**
Подготовка к сдаче и сдача экзамена	**-**	**-**	**-**	**-**	**16**	**16**
Итого по дисциплине	**48**	**-**	**48**	**48**	**36**	**180**
	96					

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

6. Лабораторные занятия (работы)

Лабораторные занятия учебным планом не предусмотрены

7. Практические занятия

Таблица 3 – Практические занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ПЗ	Количество часов ПЗ
Семестр – А (48 час.)			
1.	Тема 1	Анализ рисков информационной безопасности	6
2.	Тема 2	Построение концепции информационной безопасности предприятия	6
3.	Тема 2	Процедура аутентификации пользователя на основе пароля	6
4.	Тема 3	Тестирование защищенности транспортного уровня	6
5.	Тема 3	Механизмы контроля целостности данных	6
6.	Тема 4	Тестирование защищенности механизма управления доступом	6
7.	Тема 4	Тестирование защищенности механизма управления сессиями	6
8.	Тема 5	Тестирование на устойчивость к атакам отказа в обслуживании	6
Всего за семестр:			48
Итого по дисциплине			**48**

8. Самостоятельная работа студента

Таблица 4 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СР	Количество часов СР	Форма контроля, аттестации
Семестр – А (48 час.)			
1.	ГОСТР ИСО/МЭК 15408–2—2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 2 Функциональные компоненты безопасности	8	конспект лекций устный опрос
2.	Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Технологии создания отказоустойчивых систем.	8	конспект лекций устный опрос
3.	Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (РД 50-34.698-99).	8	конспект лекций устный опрос

4.	Конструкторская, эксплуатационная документация по ТСОИ и ПО (ГОСТ 19.101-77 и ГОСТ 2.601-2013).	8	конспект лекций устный опрос
5.	Диагностические программы и пакеты диагностических программ, предназначенные для построения систем защиты АС, обрабатывающих конфиденциальную информацию и персональные данные.	8	конспект лекций устный опрос
6.	Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств защищенных АС.	8	конспект лекций устный опрос
Всего за семестр:		**48**	
Итого по дисциплине		**48**	

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

9.1. Нормативно-правовые акты:

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 5 декабря 2016 г. № 646.
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // «Собрание законодательства РФ», 14.04.2014, N 15, ст. 1691.
3. Федеральный закон Российской Федерации от 28 декабря 2010 г № 380 - ФЗ "О безопасности".
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне»
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. ГОСТ Р ИСО/МЭК 7498-1-99 Взаимосвязь открытых систем базовая эталонная модель Часть 1 Базовая модель
9. ГОСТ 24.104-85 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Автоматизированные системы управления. Общие требования
10. ГОСТ 24.202-80. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документа «Технико-экономическое обоснование»
11. ГОСТ 24.205-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по информационному обеспечению
12. ГОСТ 24.206-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по техническому обеспечению
13. ГОСТ 24.207-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по программному обеспечению
14. ГОСТ 24.208-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов стадии «Ввод в эксплуатацию»
15. ГОСТ 24.209-80 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по организационному обеспечению

16. ГОСТ 24.210-82 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов по функциональной части

17. ГОСТ Р ИСО/МЭК 15408-2-2002 Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий Часть 2 Функциональные требования безопасности

18. ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности».

19. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

20. ГОСТ Р ИСО/МЭК ТО 19791-2008. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем», Госстандарт России

21. ГОСТ Р ИСО/МЭК 27005-2009 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», Госстандарт России

22. ГОСТ 29339-92. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования».

23. ГОСТ Р 50739-95. «СВТ. Защита от несанкционированного доступа к информации. Общие технические требования».

24. ГОСТ Р 50752-95. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний».

25. ГОСТ Р 50922-96. «ЗИ. Основные термины и определения»

26. Руководящий документ. «АС. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1998 г.

27. Руководящий документ. «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998 г.

28. Приказ ФСТЭК России от 31 августа 2010 г. N 489 — устанавливает требования к защите информации, обрабатываемой в ИС общего пользования;

29. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 — содержит требования об обработке и защите информации, не являющейся гостайной, в ГИС;

30. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 — регламентирует защиту персональных данных при обработке их в ИС: устанавливает перечень мер безопасности и раскрывает их содержание;

31. Приказ ФСТЭК России от 14 марта 2014 г. N 31 — регламентирует работу по защите информации в АС, управляющими опасными производственными и технологическими процессами на важных и потенциально опасных объектах.

9.2 Основная учебная литература

1. Разработка и эксплуатация автоматизированных информационных систем : учебное пособие / Л. Г. Гагарина, Д. В. Кисилев, Е. Л. Федотова. - М. : ИД "Форум", 2009. - 384 с. (наличие в библиотеке БГАРФ - 15 экз.)

2. Управление рисками информационной безопасности : учебное пособие / Н. Г. Милославская, М.Ю. Сенаторов, А. И. Толстой. - М. : Горячая линия - Телеком, 2012. - 130 с. (наличие в библиотеке БГАРФ - 17 экз.)

9.3. Дополнительная учебная литература

1. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. - М. : ИД "Форум" ; М. : ИНФРА-М, 2013. - 416 с. (наличие в библиотеке БГАРФ - 20 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. Защита информации в персональном компьютере : учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. - М. : Форум, 2013. - 368 с. (наличие в библиотеке БГАРФ - 25 экз.)

4. Проектирование информационных систем : учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. - М. : Форум, 2013. - 432 с. (наличие в библиотеке БГАРФ - 12 экз.)

9.4. Периодические издания

1. Защита информации. Инсайд : информационно-методический журнал. - СПб. : ООО "Изд. Дом "Афина".

2. Радиотехника : международный научно-технический журнал. - М. : ЗАО "Издательство "Радиотехника".

3. Вопросы радиоэлектроники : научный журнал. - М. : АО "ЦНИИ "Электроника".

4. Безопасность информационных технологий : научно-технический журнал. - М. : Изд-во журнала "Безопасность информационных технологий".

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 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 «Разработка и эксплуатация защищенных автоматизированных систем».

13. Особенности преподавания и освоения дисциплины

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы.

Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение практических 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 «Разработка и эксплуатация защищенных автоматизированных систем» — 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.

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий.

14.2. Виды занятий и способы контроля

В соответствии с рабочим учебным планом дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» включает следующие виды занятий: лекции, практические занятия, самостоятельная работа студентов.

При проведении лекционных занятий целесообразно широко применять такую форму как лекция-визуализация, сопровождая изложение теоретического материала презентациями, при этом желательно заблаговременно обеспечить студентов раздаточным материалом. 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.

Основной упор в методике проведения занятий сделан на сочетание лекционных и практических занятий, проводимых на средствах вычислительной техники в специально оборудованном классе. При этом изучаемый учебный материал практически отрабатывается и закрепляется слушателями в процессе работы на средствах вычислительной техники в ходе выполнения лабораторных работ.

Практические занятия направлены на закрепление лекционного материала. При подготовке к занятиям руководствоваться и «Методическими указаниями по выполнению практических работ по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем».

В заключительной части лекции необходимо делать выводы и ставить задачи на самостоятельную работу.

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.

Для более глубокого изучения теоретических вопросов слушателям предлагается выполнить долгосрочное индивидуальное задание, целью которого является проведение отдельных этапов проектирования автоматизированной информационной системы в соответствии с вариантом из перечня актуальных тем, формируемых преподавателем.

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 «Разработка и эксплуатация защищенных автоматизированных систем».

Текущий контроль усвоения знаний осуществляется путем подготовки и сдачи отчетов по итогам проверки выполнения индивидуального задания, опросов на практических занятиях.

На изучение дисциплины отводятся один семестр. Итоговая отчетность по дисциплине – экзамен. Целесообразно осуществлять проведение экзамена в форме устного опроса по билетам.

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./