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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(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

Дисциплина "Управление информационной безопасностью" имеет целью изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности в организации (на предприятии).

1.2 Задачи дисциплины:

- формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем (АС);
- выявление возможных способов нарушения информационной безопасности при работе автоматизированных систем обработки информации;
- в рамках задач обеспечения информационной безопасности решение вопросов использования радиоэлектронной аппаратуры и других технических средств;
- применение системного подхода к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер, учитывающих особенности функционирования предприятия и решаемых им задач;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность.

1.3 Место дисциплины в структуре профессиональной подготовки выпускников.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты освоения:

1) Знать:

• современные подходы к управлению ИБ и направлениях их развития;

• основные стандарты, регламентирующие управление ИБ;

• принципы разработки процессов управления ИБ;

• взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;

• подходы к интеграции СУИБ в общую систему управления предприятием.

2) Уметь:

• анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;

• определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;

• применять процессный подход к управлению ИБ в различных сферах деятельности;

• используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность.

3) Владеть:

• навыками управления информационной безопасностью простых объектов;

• терминологией и процессным подходом построения систем управления ИБ;

• навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

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
ОК-4: способность использовать основы правовых знаний в различных сферах деятельности	**Знать**		**Знать:** основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации **Уметь:** использовать в практической деятельности правовые знания **Владеть:** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
	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	

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 **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	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		
	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-3: способность проводить анализ защищенности автоматизированных систем	**Знать**		**Знать:** требования к шифрам и основные характеристик шифров; модели шифров и математические методы и исследования; программно-аппаратные средства обеспе чения информационной безопасности в типовых опера ционных 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
	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 пере-	

		чень исследуемых систем	**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 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, 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.
	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	
	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 информации. **Уметь:** определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации **Владеть: м**етодикой определения отказоустойчивости автоматизированных систем; методикой выявления
	Уровень 1	порядок разработки, внедрения и эксплуатации автоматизированных систем, отвечающих требованиям информационной безопасности	
	Уровень 2	организацию обеспечения информационной безопасности при эксплуатации защищенных АС	
	Уровень 3	основные средства анализа защищенности автоматизированных систем	
	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		уязвимостей информационных систем; методикой определения эффективности предложенных решений с учетом снижения рисков
	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-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-13: способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать**		**Знать:** методы проектирования средств защиты информации **Уметь:** разрабатывать и исследовать модели информацион-
	Уровень 1	принципы и правила построения защищенных автоматизированных систем предприятия (организации)	
	Уровень 2	формальные модели безопасности и основные принципы построения модели защиты АС	

	Уровень 3	основные принципы и методы планирования функционирования защищенных автоматизированных систем	но-технологических ресурсов, проектировать средств защиты информации **Владеть:** методами исследования информационно технологических ресурсов, методами проектирования средст 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-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-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
	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	**Владеть**: способами, механизмами способы и механизмы управления информационной безопасностью автоматизированной системы
	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-7.2: способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных систем	**Знать**		**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах. **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**: 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
	Уровень 1	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации	
	Уровень 2	способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
	Уровень 3	принципы построения систем защиты информации	
	Уметь		
	Уровень 1	классифицировать и оценивать угрозы безопасности информации для объекта информатизации	
	Уровень 2	разрабатывать предложения по совершенствованию системы управления информационной безопасностью АС	
	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.32 «Управление информационной безопасностью» 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» – знать основы права и законодательства России, уметь использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; владеть навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.

«Основы информационной безопасности» – знать сущность и понятие ИБ и характеристику ее составляющих, источники и классификацию угроз ИБ, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

«Безопасность жизнедеятельности» – знать опасные и вредные факторы системы «человек – среда обитания»; уметь реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности, применять основные методы защиты производственного персонала и населения от возможных последствий аварий; владеть навыками безопасного использования технических средств в профессиональной деятельности.

«Основы управленческой деятельности" – знать научные основы, цели, принципы, методы и технологии управленческой деятельности; уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность; владеть навыками выбора, обоснования, реализации и контроля результатов управленческого решения.

«Программно-аппаратные средства обеспечения информационной безопасности» – знать программно-аппаратные средства обеспечения информационной безопасности; 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 использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;

«Разработка и эксплуатация защищенных автоматизированных систем» – знать методы, способы, средства, последовательность и содержание этапов разработки подсистем безопасности АС, основные меры по защите информации в автоматизированных системах, криптографические методы, используемые для обеспечения ИБ в АС; уметь администрировать подсистемы информационной безопасности автоматизированных систем, исследовать эффективность создаваемых средств автоматизации; владеть методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем, навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками анализа информационной инфраструктуры безопасности АС.

Дисциплина необходима для освоения преддипломной практики. В свою очередь, данная дисциплина является обеспечивающей для написания выпускной квалификационной работы.

4. Содержание дисциплины

Тема 1. Введение

Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Содержание и задачи процесса управления ИБ АС и предприятия в целом.

Тема 2. Система управления информационной безопасностью автоматизированных систем

Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии. Стандартизация в сфере управления ИБ (на основе международных стандартов ISO/IEC 17799, ISO/IEC 27002, ISO/IEC 27001, ISO/IEC 15408). Ресурсы предприятия, подлежащие защите с точки зрения ИБ. Комплекс методов и средств защиты информации как объект управления ИБ.

Тема 3. Политика безопасности автоматизированных систем

Перечень нормативно-методических и организационно-распорядительных документов по защите информации на предприятии. Концепция безопасности предприятия и ИБ. Назначение и содержание политики ИБ предприятия в целом, его структурных подразделений, частных политик безопасности. Средства их реализации. Модель нарушителя политики безопасности. Типичные угрозы информации и уязвимости корпоративных АС. Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.

Тема 4. Организация обеспечения информационной безопасности автоматизированных систем

Состав, роль, место и особенности взаимодействия субъектов процесса управления ИБ АС. Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии. Организация контроля эффективности выполнения персоналом, ответственным за ИБ, своих функциональных обязанностей.

Тема 5. Аудит информационной безопасности автоматизированных систем

Назначение, цели и виды аудита ИБ АС. Требования к аудитору ИБ, особенности взаимодействия между аудитором и заказчиком. Оценка работы аудитора. Стандартизация в сфере аудита ИБ. Содержание и организация процесса аудита ИБ. Оценка рисков ИБ. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита ИБ.

Тема 6. Средства поддержки процессов управления информационной безопасностью АС

Выбор необходимых программных и программно-аппаратных средств защиты информации в АС, проектирование комплексной системы защиты информации предприятия эффективной с точки зрения решаемых задач и необходимых для этого ресурсов. Программные средства автоматизации процедур проведения аудита ИБ и анализа политики ИБ. Программные средства поддержки процессов управления ИБ.

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 (4 ЗЕТ, 144 час.)						
Тема 1. Введение.	4	-	-	4	-	**8**
Тема 2. Система управления информационной безопасностью автоматизированных систем.	6	-	8	6	-	**20**
Тема 3. Политика безопасности автоматизированных систем.	6	-	8	10	-	**26**
Тема 4. Организация обеспечения информационной безопасности автоматизированных систем.	6	-	8	10	-	**26**
Тема 5. Аудит информационной безопасности автоматизированных систем.	8	-	16	10	-	**28**
Тема 6. Средства поддержки процессов управления информационной безопасностью АС.	6	-	8	10	-	**26**
Всего	**36**	**-**	**48**	**50**	**-**	**134**
Подготовка к сдаче и сдача зачета с оценкой	**-**	**-**	**-**	**10**	**-**	**10**
Итого по дисциплине	**36**	**-**	**48**	**60**	**-**	**144**
	84					

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 2	Нормативное обеспечение управления рисками информационной безопасности	4
2.	Тема 2	Исследование требований нормативных документов по защите информации к стойкости парольной защиты	4
3.	Тема 3	Сравнительный анализ моделей организационного управления информационной безопасностью	8
4.	Тема 4	Функциональных обязанности работников подразделения информационной безопасности	8
5.	Тема 5	Изучение методики анализа рисков информационной безопасности	8
6.	Тема 5	Организация изолированных пользовательских сред	8
7.	Тема 6	Secret Net. Замкнутая программная среда. Контроль целостности	8
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 (60 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	6	конспект лекций устный опрос
2	Угрозы информационной безопасности в информационных системах	6	конспект лекций
3	Стандарты управления информационной безопасностью - BS 7799 и ISO/IEC 17799. Их основные положения	6	конспект лекций устный опрос
4	Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	6	конспект лекций устный опрос
5	Создание СУИБ на предприятии (этапы создания, категорирование активов, оценка защищенности информационной системы, оценка информационных рисков)	6	конспект лекций устный опрос
6	Методика оценки рисков информационной безопасности компании	6	конспект лекций устный опрос
7	Методики и технологии управления рисками	6	конспект лекций устный опрос

8	Разработка корпоративной методики анализа рисков	6	конспект лекций
9	Современные методы и средства анализа и управление рисками информационных систем компаний	6	конспект лекций устный опрос
10	Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика	6	конспект лекций устный опрос
Всего за семестр:		**60**	
Итого по дисциплине		**60**	

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. Основы управления информационной безопасностью : учебное пособие / А.П. Курило [и др.]. - М. : Горячая линия - Телеком, 2012. - 244 с (наличие в библиотеке БГАРФ - 20 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. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие / Н. Г. Милославская, М.Ю. Сенаторов , А. И. Толстой. - М. : Горячая линия - Телеком, 2012. - 214 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. 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 практических 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 «Управление информационной безопасностью».

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 зачету 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

Изучение дисциплины "Управление информационной безопасностью" является одной из завершающих стадий прикладной подготовки специалистов в области обеспечения информационной безопасности автоматизированных систем. Ее освоение должно обеспечить интеграцию полученных ранее знаний в области методов и средств защиты информации с материалами по правовым и организационным аспектам ИБ АС, способность обучаемых применить приобретенные умения и навыки в своей профессиональной деятельности.

По этой причине основной упор в процессе изучения дисциплины должен быть сделан на сочетание лекционных и семинарских занятий с методами активизации познавательной деятельности обучающихся в виде подготовки рефератов по актуальным практическим ситуациям в области управления ИБ и их обсуждения в ходе семинарских занятий. Дополнительно изучаемый учебный материал в части освоения соответствующих средств автоматизации процессов управления ИБ АС должен отрабатываться и закрепляться на практических занятиях.

14.2. Виды занятий и способы контроля

В соответствии с рабочим учебным планом дисциплина «Управление информационной безопасностью» 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 «Управление информационной безопасностью».

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 «Управление информационной безопасностью».

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 – зачет с оценкой.

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./