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

«26» 06 2018 г.

РАБОЧАЯ ПРОГРАММА

«Производственная - Преддипломная практика»

(наименование практики)

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

1. Тип, способ проведения, базы и цель прохождения практики

1.1 **Тип практики**: преддипломная практика.
1.2 **Способ проведения практики**: стационарная, выездная.
Форма проведения практики: дискретно.
1.3 **Целями преддипломной практики** являются:

- приобретение навыков работы в реальной производственной среде на основе теоретических знаний, полученных студентами по специальности 10.05.03 «Информационная безопасность автоматизированных систем»;
- освоение студентами практических навыков работы с нормативно-правовой базой деятельности в области обеспечения информационной безопасности автоматизированных систем;
- закрепление 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;
- 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 автоматизированных систем.

1.4 **Задачи** практики:

- ознакомление со структурой подразделения, в котором проходит практика, его функциями и связями с другими подразделениями предприятия;
- изучение организации проектных работ;
- приобретение практических навыков на рабочем месте специалиста по защите информации;
- ознакомление с видами документации, стандартами и другими нормативными документами в области информационной безопасности;
- закрепление знаний и выработка умений по проектированию средств защиты информации, составлению и использованию программного обеспечения и т.п.;
- выработка умений и навыков при работе на автоматизированном рабочем месте;
- выработка навыков творческого подхода к решению теоретических и практических задач по специальности;
- сбор, обобщение и систематизация материалов для выпускной квалификационной работы в соответствии с темой;
- выработка умений оценки технико-экономических показателей выполняемого проекта (работы) в соответствии с действующими нормативно-техническими документами.

Преддипломная практика способствует формированию и развитию у обучающихся следующих общепрофессиональных, профессиональных, профессионально-специализированных компетенций:

- ОПК-8: способностью к освоению новых образцов программных, технических средств и информационных технологий;
- ПК-1: способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
- ПК-3: способностью проводить анализ защищенности автоматизированных систем;
- ПК-6: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
- ПК-7: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

- ПК-11: способностью разрабатывать политику информационной безопасности автоматизированной системы;
- ПК-13: способностью участвовать в проектировании средств защиты информации автоматизированной системы;
- ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-18: способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
- ПК-21: способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
- ПК-23: способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
- ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы;
- ПК-28: способностью управлять информационной безопасностью автоматизированной системы;
- ПСК-7.1: способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
- ПСК-7.2: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах;
- ПСК-7.4: способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
- ПСК-7.5: способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации.

Преддипломная практика проводится в профильных организациях с проблематикой в области защиты информации (предприятиях, учреждениях, НИИ, организациях и учреждениях различной организационно-правовой формы) или, в качестве исключения, на кафедрах и в научных лабораториях БГАРФ ФГБОУ ВО «КГТУ». Места прохождения преддипломной практики определяются двухсторонними договорами па прохождение преддипломной практики студентов от организаций. Места прохождения преддипломной практики могут выбираться студентами самостоятельно при содействии вуза и руководителя практики.

Преддипломная практика представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся в соответствии с графиком учебного процесса и временем ее проведения.

2. Результаты прохождения практики

Прохождение преддипломной практики направлено на овладение общепрофессиональными компетенциями (ОПК), профессиональными компетенциями (ПК) и профессионально-специализированными компетенциями (ПСК) предусмотренными образовательной программой (ОП).

Планируемые результаты прохождения по преддипломной практике, соотнесенные с планируемыми результатами освоения программы специалитета (компетенциями выпускников) приведены в таблице 1.

Таблица 1. - Планируемые результаты прохождения по преддипломной практике

Компетенции выпускника ОП ВО и этапы их формирования в результате прохождения практики	Знания, умения, навыки и опыт профессиональной деятельности, характеризующие этапы формирования компетенций
1	2
ОПК-8: способность к освоению новых образцов программных, технических средств и информационных технологий	**Знать:** принципы построения и функционирования, примеры реализаций современных операционных систем; основы теории электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры **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; применять на практике методы анализа электрических цепей; работать с современной элементной базой электронной аппаратуры **Владеть:** навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы
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:** 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
ПК-3: способность проводить анализ защищенности автоматизированных систем	**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
ПК-6: способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Знать:** требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные информационные технологии, используемые в автоматизированных системах;

	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; **Уметь:** анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; **Владеть:** навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; профессиональной терминологией в области информационной безопасности; навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-7: способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**Знать:** принципы построения и функционирования, примеры реализаций современных операционных систем **Уметь:** разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; 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 разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации; навыками участия в экспертизе состояния защищенности информации на объекте защиты
ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы	**Знать:** основные задачи и понятия криптографии; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. **Владеть:** навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
ПК-13: способность участвовать в проектировании средств защиты информации автоматизированной системы	**Знать:** требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, крипто-

	графические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах **Уметь:** применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. **Владеть:** криптографической терминологией; методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации.
ПК-14: способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** требования к шифрам и основные характеристики шифров; основные информационные технологии, используемые в автоматизированных системах **Уметь:** контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем **Владеть:** навыками участия в экспертизе состояния защищенности информации на объекте защиты; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; методами расчета и инструментального контроля показателей технической защиты информации; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков.
ПК-18: способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**Знать:** основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; содержание управленческой работы руководителя подразделения; проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем **Уметь:** оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; проводить мониторинг угроз безопасности компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик 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

ПК-21: способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем **Владеть:** навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности
ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**Знать:** основные задачи и понятия криптографии; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных 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:** методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов
ПК-26: способность администрировать подсистему информационной безопасности автоматизированной системы	**Знать:** технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; источники и классификацию угроз информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; **Уметь:** планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; администрировать подсистемы информационной безопасности автоматизированных систем **Владеть:** навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; 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; навыками работы с технической документацией на ЭВМ и вычислительные системы; профессиональной терминологией в области информационной безопасности; 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; навыками разработки программной документации

ПК-28: способность управлять информационной безопасностью автоматизированной системы	**Знать:** основные методы управления информационной безопасностью **Уметь:** разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем **Владеть:** методами управления информационной безопасностью автоматизированных систем
ПСК-7.1: способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую ин формацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы **Владеть:** владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов
ПСК-7.2: способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы **Владеть:** владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов
ПСК-7.4: способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы **Владеть:** владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов
ПСК-7.5: способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации	**Знать:** обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности. **Уметь:** на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет;

	формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы **Владеть:** владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов

3. Место практики в структуре ОП

Преддипломная практика (Б2.Б.04 (Пд)) проводится в соответствии с утвержденным рабочим учебным планом и календарным графиком учебного процесса.

Для освоения преддипломной практики, обучающиеся должны обладать знаниями, умениями и навыками, полученными в результате формирования и развития компетенций в следующих дисциплинах:

Философия, История Отечества, Иностранный язык, Правоведение, Экономика, Основы управленческой деятельности, Алгебра и геометрия, Математический анализ, Дискретная математика, Теория вероятностей и математическая статистика, Математическая логика и теория алгоритмов, Теория информации, Информатика, Физика, Исследование операций и теории игр, Теория графов и ее приложения, Безопасность жизнедеятельности, Языки программирования, Технологии и методы программирования, Электроника и схемотехника, Безопасность операционных систем, Безопасность сетей электронных вычислительных машин, Безопасность систем баз данных, Основы информационной безопасности, Криптографические методы защиты информации, Организация электронных вычислительных машин и вычислительных систем, Техническая защита информации, Сети и системы передачи информации, Организационное и правовое обеспечение информационной безопасности, Программно-аппаратные средства обеспечения информационной безопасности, Разработка и эксплуатация защищенных автоматизированных систем, Управление информационной безопасностью, Инженерная графика, Информационная безопасность распределенных информационных систем, Методы проектирования защищенных распределенных информационных систем, Технология построения защищенных распределенных приложений, Физическая культура и спорт, Профессиональный английский язык, Компьютерные сети, Информационная безопасность автоматизированных информационных систем, Программирование средств защиты информации, Комплексное обеспечение информационной безопасности автоматизированных систем, Теоретические основы компьютерные безопасности, Русский язык и культура речи, Политология, Психология и педагогика, Пакеты прикладных программ, Экспертные системы, Цифровые средства обработки информации, Системы защиты от утечки конфиденциальной информации.

Проведение преддипломной практики предоставляет необходимые знания для выполнения выпускной квалифицированной работы.

4. Объем (трудоемкость) и продолжительность практики, формы аттестации по ней

Объем практики: 18 з.е. (648 ч.) после семестра А обучения

Таблица 2. – Продолжительность практики, формы аттестации

Разделы (этапы) преддипломной практики и их содержание	Объем раздела (этапа) час.			Формируемые компетенции	Формы контроля, аттестации
	Всего	учебные занятия	самостоятельная работа студента		
1. Подготовительный этап	162	8	154	ОПК-8, ПК-18	Промежуточная аттестация
2. Производственный этап	186	8	178	ОПК-8, ПК-1, ПК-3, ПК-6, ПК-7, ПК-11, ПК-13, ПК-14, ПК-18, ПК-21, ПК-23, ПК-26, ПК-28, ПСК-7.1, ПСК-7.2, ПСК-7.4, ПСК-7.5	Промежуточная аттестация
3. Обработка и анализ полученной информации	200	8	192	ПК-1, ПК-6, ПК-7, ПК-18, ПК-21, ПК-23, ПСК-7.5	Промежуточная аттестация
4. Подготовка отчета по преддипломной практике	100	-	100	ПК-7	Промежуточная аттестация
ИТОГО	**648**	**24**	**624**		Дифференцированный зачет по отчету по практике

5. Содержание практики

Таблица 3. – Содержание преддипломной практики

№ п/п	Разделы (этапы) практики	Виды преддипломной работы на практике, включая самостоятельную работу и трудоемкость (в часах)				Формы контроля
		ознакомительные мероприятия	инструктаж	сбор и обработка материала	подготовка отчета	
1	Инструктаж по требованиям техники безопасности, охране труда и пожарной безопасности. Инструктаж по правилам внутреннего трудового распорядка организации. Доведения порядка прохождения преддипломной практики и вида отчетности за практику.		4			проверка знаний по итогам инструктажа
2	Поиск, сбор и обработка информации о предприятии в сфере профессиональной деятельности.	2		62	15	параграф в отчете
3	Описание организационной структуры выбранного предприятия в сфере профессиональной деятельности.	2		62	15	параграф в отчете
4	Определение круга управленческих и аналитических задач, решаемых в рамках выбранного подразделения, и формирование общего представления об информационной безопасности предприятия.	2		45	13	параграф в отчете

5	Изучение организационно-правовых документов, регламентирующих юридический статус организации, его организационно-правовую форму: устав (положение) организации, положения о структурных подразделениях и т.д.	2		45	15	параграф в отчете
6	Изучение принятой в организации системы защиты информации, комплекса проводимых организационно-профилактических мероприятий по предупреждению несанкционированной утечки конфиденциальной информации.	2	2	45	15	параграф в отчете
7	Сбор, систематизация и обработка собранного материала	2		142	50	
8	Оформление и представление (каждого индивидуально) рабочих материалов и результатов практической работы в форме отчетов о практике, а также отзывы с оценками работы со стороны руководителей от предприятий (организаций)	6		70	30	публичная защита итогового отчета по практике, презентация доклада, дифференцированный зачет
	ИТОГО:	**18**	**6**	**471**	**153**	**648**

5.1. Соответствие компетенций, формируемых при прохождении практики

Таблица 4 – Соответствие компетенций и видов занятий, формируемых при прохождении практики

Виды занятий			
формируемые компетенции	**учебные занятия**	**самостоятельная работа студента**	**Форма контроля**
ОПК-8	+	+	проверка календарного плана работ; проверка промежуточных отчетов; сдача инструктажа по технике безопасности, охране труда и пожарной безопасности; сдача инструктажа по правилам внутреннего трудового распорядка организации; собеседование с руководителем
ПК-1	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-3	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-6	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-7	+	+	проверка дневника по практике; проверка календарного плана работ; проверка промежуточных отчетов; презентация доклада; публичная защита итогового отчета по практике; оценка по результатам защиты отчета
ПК-11	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-13	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-14	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-18	+	+	проверка календарного плана работ; проверка промежуточных отчетов; сдача инструктажа по технике безопасности, охране труда и пожарной безопасности; сдача инструктажа по правилам внутреннего трудового распорядка организации; собеседование с руководителем
ПК-21	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем

ПК-23	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-26	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПК-28	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПСК-7.	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПСК-7.2	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПСК-7.4	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем
ПСК-7.5	+	+	проверка календарного плана работ; проверка промежуточных отчетов; собеседование с руководителем

6. Формы и требования к отчетности по практике

Прохождение преддипломной практики состоит из практической деятельности студента. Вопросы, порядок их изучения и выполнения практической работы выдаются до начала преддипломной практики руководителем выпускной квалификационной работы студента.

Во время прохождения преддипломной практики производится изучение выданных руководителем выпускной квалификационной работы вопросов.

Во время прохождения преддипломной практики студент должен вести дневник, в котором описывается выполненная за день работа, указывается, в какой форме она была исполнена (самостоятельно, под наблюдением руководителя преддипломной практики от организации, на основе изучения архивных материалов и т.п.). В дневнике отмечается также присутствие на производственных совещаниях, научно-исследовательская работа в период практики. Запись в дневнике ежедневно проверяется и подписывается непосредственным руководителем практики от организации. Руководитель практики, должен контролировать правильность оформления и соответствия работ заданию практики не реже одного раза в две недели.

По итогам преддипломной практики должен быть подготовлен отчёт, в котором следует отразить проделанную работу при выполнении задания преддипломной практики, приложить документы, подтверждающие обоснованность сделанных выводов. Отчет по практике составляется в соответствии с требованиями программы и с учетом индивидуального задания, выданного студенту перед началом практики. При этом описание предлагаемых работ, записи в дневнике, последующие выводы и предложения должны быть взаимоувязаны. Отчёты, не отвечающие этому требованию, к сдаче не допускаются. Таким образом, отчёт по преддипломной практике должен представлять собой полную характеристику работы студента-практиканта в организации.

Работа по составлению отчёта проводится студентом систематически на протяжении всего периода практики. После завершения работ по той или иной теме студент обрабатывает накопившийся материал, последовательно излагает его и представляет его на проверку руководителю практики. В конце практики отчёт оформляется окончательно.

Достоинством отчёта по преддипломной практике является наличие аналитического материала, полнота освещения вопросов, глубокое знание предмета защиты. Следует отметить, что анализ должен содержать изложение всех вопросов, представленных в задании практики, а также вопросов, дополнительно поставленных руководителем выпускной квалификационной работы. Отчёт о прохождении преддипломной практики должен не только по содержанию, но и по форме отвечать предъявленным требованиям.

В 3-дневный срок после прибытия студентов с практики в академию отчеты по практике должны быть сданы руководителю практики на проверку. Вместе с отчетами руководителю практики сдаются также характеристики, дневники практики и направления на практику.

В 30-дневный срок после возвращения студента с практики отчеты должны быть защищены у руководителя практики от академии. Допускается защита отчетов в последнюю

неделю практики, а по практикам, проводимым в летнее время года – в течение первого месяца семестра, следующего за практикой. В процессе защиты студент должен кратко изложить основные результаты проделанной работы, выводы и рекомендации, структуру и анализ материалов, включаемых в дипломную работу, оценить их полноту. Основным критерием при оценке отчета о преддипломной практике является наличие в нём материалов, позволяющих на их основе качественно подготовить и защитить выпускную квалификационную работу, наличие аналитической части, выявленных проблемах организации и конкретных предложений по их эффективному решению.

Результаты защиты отчетов отражаются в зачетных книжках и в ведомости в соответствии с рабочим учебным планом (с оценками по шкале – отлично, хорошо, удовлетворительно, неудовлетворительно, либо зачет – незачет).

Студенты, не выполнившие программу практики по уважительным причинам, направляются на практику в свободное от учебы время, в объеме часов, предусмотренных учебным планом. Студенты, не выполнившие программу практики без уважительной причины, или получившие неудовлетворительную оценку за практику, подлежат отчислению из академии за академическую неуспеваемость.

Студенты, не защитившие отчеты по практике по истечении первого месяца учебного семестра, следующего за практикой, подлежат отчислению из академии за академическую неуспеваемость.

7. Учебно-методическое обеспечение практики

7.1 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 29339-92. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования».
9. ГОСТ Р 50739-95. «СВТ. Защита от несанкционированного доступа к информации. Общие технические требования».
10. ГОСТ Р 50752-95. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний».
11. ГОСТ Р 50922-96. «ЗИ. Основные термины и определения»
12. Руководящий документ. «АС. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1998 г.
13. Руководящий документ. «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998 г.

7.2 Основная 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. Зайцев, А.П. Техническая защита информации : учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М. : Горячая линия-Телеком, 2009. – 616 с. (наличие в библиотеке БГАРФ - 17 экз.)

3. 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.)

4. 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 - 29 экз.)

7.3 Дополнительная литература:

1. Информационная безопасность судовых радиолокационных систем [Текст] : конспект лекций для курсантов и студентов радиотехнического факультета академии / О. П. Пономарев ; Федеральное агентство по рыболовству, БГАРФ. - Калининград : Изд-во БГАРФ. Ч.1 : Общие сведения о радиолокации. - 2012. - 103 с. (наличие в библиотеке БГАРФ - 160 экз.)

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М. : ИД «Форум», 2013. – 416 с. (наличие в библиотеке БГАРФ - 20 экз.)

3. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А. Клейменов. – Москва: Академия, 2008. – 336 с. (наличие в библиотеке БГАРФ - 31 экз.)

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

5. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин [и др.] ; Академия следственного комитета Российской Федерации. - М. : ЮНИТИ-ДАНА, 2017. - 287 с.

6. 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.)

8. Информационные технологии, используемые для проведения практики, включая перечень программного обеспечения и информационно-справочных систем, а также Интернет-ресурсы:

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.

9. Материально-техническая база практики

Преддипломная практика студентов могут проходить в любых организациях, где используются технические средства обработки, хранения и передачи конфиденциальной ин-

формации, а именно: органах государственной власти, силовых структурах (МВД, ФСБ, ГИБДД, МЧС, таможенной службе, налоговых органах), медицинских учреждениях, банках и других финансовых организациях, на предприятиях промышленности, энергетики, торговли, связи и транспорта, а также в научно-исследовательских институтах, на кафедрах и в лабораториях вуза.

Материально-техническое обеспечение практики должно быть достаточным для достижения целей практики, соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных, научно-производственных и других работ.

Материально-техническая база должна обеспечить возможность доступа обучающихся к информации, необходимой для выполнения задания по практике и написанию отчета. Рабочее место обучающегося обеспечено компьютерным оборудованием в объемах, достаточных для достижения целей практики. Во время прохождения практики обучающийся использует современную аппаратуру и средства обработки данных (компьютеры, информационные системы и пр.), которые соответствуют требованиям выполнения заданий на практике. Для выполнения индивидуальных заданий на практику, оформления отчета о выполнении индивидуальных заданий обучающимся доступна электронная образовательная среда образовательной организации: серверы на базе MS SQL Server, файловый сервер с электронным образовательным ресурсом, базами данных позволяют обеспечить одновременный доступ обучающихся к электронной информационно-образовательной среде, к электронному образовательному ресурсу, информационно-образовательному ресурсу; компьютеры с выходом в сеть Интернет обеспечивают доступ к электронной информационно-образовательной среде организации.

Студент обеспечивается рабочим местом в соответствии с получаемой специальностью, одновременно создаются необходимые условия для самостоятельного сбора в период практики информации по организации производства, технике и технологий, информационному обеспечению, программному обеспечению, методах, средствах защиты информации, функциям подразделений по защите информации и т.д. Предоставляется студенту возможность и обеспечение доступа к необходимой для исследования информации, находящейся на электронных носителях (ПК, локальные компьютерные сети, оборудование защиты информации и т.п.).

База практики должна обладать следующим минимально необходимым материально-техническим обеспечением:

- кабинеты (рабочее место) - ауд. 255 – «Центр информационных технологий» БГАРФ ФГБОУ ВО «КГТУ», ауд. 431 (1) – кабинет для самостоятельной работы, ауд. 434 – помещение для хранения и профилактического обслуживания учебного оборудования;
- необходимые правовые документы и рабочие материалы;
- измерительные и вычислительные комплексы;
- специализированное лицензионное программное обеспечение;
- СПС «Консультант Плюс», «Гарант».

Помещения оборудованы персональными компьютерами с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду всего университетского комплекса (ООО «ЭБС ЛАНЬ» - договор № 22/18АО от 24.04.2018). Комплект лицензионного программного обеспечения (Интернет-версия «Гарант» - договор № 04/19АО от 29.01.2019 г.; НЭБ РФ - Национальная электронная библиотека НЭБ – договор 101/НЭБ/2366 от 19.08.2017 г.; ЭБС «Университетская библиотека онлайн» - контракт № 06 от 11.03.2019 г.; ЭБС IPRbooks ООО «Ай Пи Медиа» - контракт № 4228/18 от 04.06. 2018 г. – 15.07.2019 г.).

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ПО ПРАКТИКЕ

Фонд оценочных средств (ФОС) – комплект методических и контрольных материалов, предназначенных для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей основной образовательной программы подготовки специалистов, позволяющих оценить знания, умения и уровень приобретенных компетенций.

ФОС является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися ОП ВО в свете компетентностного подхода. ФОС систематизирует и обобщает различные аспекты, связанные с оценкой качества образования, уровня сформированности компетенций обучающихся и выпускников на соответствие требованиям стандарта.

ФОС формируется на основе ключевых принципов оценивания:

– валидности (объекты оценки должны соответствовать поставленным целям обучения);

– надежности (использование единообразных стандартов и критериев для оценивания достижений);

– справедливости (разные обучающиеся должны иметь равные возможности добиться успеха);

– своевременности (поддержание развивающей обратной связи);

– эффективности (соответствие результатов деятельности поставленным задачам).

Основными свойствами ФОС являются:

– по профессиональной направленности – соответствие будущей профессиональной деятельности студента;

– по содержанию – всеобъемлющий состав и взаимосвязь оценочных средств ФОС для текущей, промежуточной аттестации;

– по объему – полнота ФОС по количественному составу оценочных средств, соответствие учебному плану направления подготовки.

– по качеству оценочных средств и ФОС в целом – объективность и достоверность результатов при проведении оценивания с различными целями.

10.1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивая

Таблица 5. – Показатели и критерии оценивания компетенций, используемые шкалы оценивания

Элементы компетенций (знания, умения, владения)	Показатели оценивания	Критерии оценивания	Средства оценивания	Шкалы оценивания
Знать (ОПК-8)	принципы построения и функционирования, примеры реализаций современных операционных систем; теоретические основы электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ОПК-8)	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 автоматизи-	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

	рованной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; применять на практике методы анализа электрических цепей; работать с современной элементной базой электронной аппаратуры			
Владеть (ОПК-8)	навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-1)	основных информационных технологий, используемые в автоматизированных системах; качественных показателей программного обеспечения; языки программирования высокого уровня (объектно-ориентированное программирование)	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-1)	применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-1)	навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-3)	требования к шифрам и основные характеристики шифров; модели шифров математические методы их исследования технические каналы утечки информации возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-3)	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	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-3)	навыками организации и обеспечения режима секретности	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2

Знать (ПК-6)	требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные информационные технологии, используемые в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-6)	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-6)	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; профессиональной терминологией в области информационной безопасности; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-7)	принципы построения и функционирования, примеры реализаций современных операционных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-7)	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; 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	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

Владеть (ПК-7)	навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации; навыками участия в экспертизе состояния защищенности информации на объекте защиты	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-11)	основные задачи и понятия криптографии; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-11)	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем.	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-11)	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-13)	требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-13)	применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем.	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

Владеть (ПК-13)	криптографической терминологией; методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации.	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-14)	требования к шифрам и основные характеристики шифров; основные информационные технологии, используемые в автоматизированных системах	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-14)	контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-14)	навыками участия в экспертизе состояния защищенности информации на объекте защиты; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков.	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-18)	основные понятия и методы в области управленческой деятельности; порядок выработки и реализации управленческих решений; содержание управленческой работы руководителя подразделения; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-18)	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; проводить мониторинг угроз безопасности компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-18)	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	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2

Знать (ПК-21)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности.	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-21)	разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-21)	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	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-23)	основные задачи и понятия криптографии; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-23)	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	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-23)	методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-26)	технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; источники и классификацию угроз информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-26)	планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; администрировать подсистемы информационной безопасности автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

Владеть (ПК-26)	навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; 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; навыками работы с технической документацией на ЭВМ и вычислительные системы; профессиональной терминологией в области информационной безопасности; 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; навыками разработки программной документации	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПК-28)	основные методы управления информационной безопасностью	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПК-28)	разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПК-28)	методами управления информационной безопасностью автоматизированных систем	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПСК-7.1)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПСК-7.1)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

Владеть (ПСК-7.1)	владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПСК-7.2)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПСК-7.2)	на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПСК-7.2)	владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПСК-7.4)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Уметь (ПСК-7.4)	на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПСК-7.4)	владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2
Знать (ПСК-7.5)	обладает фактическими и теоретическими знаниями в области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; обладает базовыми общими знаниями в области применения полученных навыков в рамках реальной практической деятельности	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1

Уметь (ПСК-7.5)	на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: дифференциальный зачет	Шкала 1
Владеть (ПСК-7.5)	владеть методами сбора и анализа данных, способностью делать обоснованные заключения на основе полученных результатов, способностью составлять и корректировать план проведения работ в зависимости от полученных результатов	Обоснованность и аргументированность выполнения учебных заданий	Текущий контроль: выполнение практического задания Промежуточная аттестация: дифференциальный зачет	Шкала 2

10.2 Описание шкал оценивания сформированности элементов компетенций

Таблица 6. – Оценка сформированности отдельных элементов компетенций (шкала 1)

Обозначения		**Формулировка требований к степени сформированности компетенции**		
Цифр.	**Оценка**	**Знать**	**Уметь**	**Владеть**
1	Неуд.	Отсутствие знаний	Отсутствие умений	Отсутствие навыков
2	Неуд.	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Удовл.	Общие, но не структурированные знания	В целом успешное, но не систематически осуществляемое умение	В целом успешное, но не систематическое применение
4	Хор.	Сформированные, но содержащие отдельные пробелы знания	В целом успешное, но содержащие отдельные пробелы умение	В целом успешное, но содержащее отдельные пробелы применение навыков
5	Отл.	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

Таблица 7. – Комплексная оценка сформированности знаний, умений и владений (шкала 2)

Обозначения		**Формулировка требований к степени сформированности компетенции**
Цифр.	**Оценка**	
1	Неуд.	Не имеет необходимых представлений о проверяемом материале
2	Удовл. или неуд. (*по усмотрению преподавателя)*	Знать на уровне ориентирования, представлений. Субъект учения знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает их в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3	Удовл.	Знать и уметь на репродуктивном уровне. Субъект учения знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4	Хор.	Знать, уметь, владеть на аналитическом уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5	Отл.	Знать, уметь, владеть на системном уровне. Субъект учения знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и

		зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

10.3 Оценочные средства результатов прохождения практик и отражение итогов практик

Итоговая оценка студенту за практику по 5-ти балльной шкале выставляется на основе накопленной им рейтинговой оценки R по итогам контроля в соответствии со шкалой:

$R=$ 86-100 баллов – «отлично»;

$R=$ 70-85 баллов – «хорошо»;

$R=$ 50-69 баллов – «удовлетворительно»;

$R<$ менее 50 баллов – «неудовлетворительно».

Значение рейтинга вычисляется по формуле

$$R= \sum_{j=1}^{7} Kij \qquad (1)$$

Значения k_{ij} определяются в соответствии с табл.8.

Таблица 8. – Рейтинговая оценка результатов практики

Показатель (*j*)	**Описание**	**Степень соответствия результатов практики требованиям, выраженная в баллах**		
		соответствует	**частично соответствует**	**не соответствует**
		k1j	***k2j***	***k3j***
1. Своевременность оформления документов практики	**Перечень оформляемых документов:** договор на прохождение практики на предприятии; письмо от предприятия; индивидуальное задание; журнал по практике; отзыв руководителя от предприятия; отзыв руководителя от кафедры.			
	Документы оформлены в срок	**14-15**		
	Документы оформлены с нарушением сроков		**7-13**	**0**
2. Отзыв руководителя от предприятия	**Оцениваются:** объем и качество проделанной работы; комплексное применение теоретических знаний на практике; самостоятельность студента в организации своей деятельности при выполнении задач практики; своевременность выполнения программы практики; умения работать в коллективе; внешний вид студента на практике.			
	Работы выполнены в полном соответствии с индивидуальным заданием	**10-15**		
	Работы выполнены не в полном соответствии с индивидуальным заданием		**5-9**	
	Работы выполнены частично с нарушением индивидуального задания			**1-4**
3. Отзыв руководителя от кафедры	**Оцениваются:** объем и качество проделанной работы; использование на практике полученных знаний в ходе учебного процесса по предметам специального цикла; применение теоретических знаний на практике; самостоятельность студента в организации своей деятельности при выполнении задач практики;			

	своевременность выполнения программы практики.			
	Работа демонстрирует высокий уровень профессиональных знаний	**10-15**		
	Работа демонстрирует средний уровень профессиональных знаний		**5-9**	
	Работа демонстрирует низкий уровень профессиональных знаний			**0**
4. Оформление отчета о прохождении практики	**Оцениваются:** стиль изложения и оформление в соответствии с требованиями стандартов; использование нормативно-правовых и нормативно-методические документов, регламентирующие деятельность организации, в которой студент проходит практику.			
	Отчёт оформлен в полном соответствии с требованиями	**5-10**		
	Отчёт оформлен с незначительными отступлениями от требований. Присутствуют замечания по стилю изложения.		**1-4**	**0**
5. Соответствие содержания отчета целям практики и образовательной программы	**Оцениваются:** полнота отражения результатов выполненной работы и поставленных задач на практику; использование современных информационных технологий, при выполнении задач практики.			
	Отчёт полно отражает результаты поставленных на практике задач с использованием современных информационных технологий	**15-20**		
	В отчёте в неполной мере отражены результаты поставленных на практике задач. Использование информационных технологий недостаточно.		**10-14**	**0**
6.Ведение дневника прохождения практики	**Оцениваются**: результаты еженедельной проверки заполнения дневника.			
	Дневник заполняется регулярно	**10**		
	Дневник заполняется не регулярно. Выявлены не значительные нарушения		**5-9**	
	Дневник заполняется не регулярно. Выявлены значительные нарушения			**1-4**
7. Соответствие содержания выполненных работ целям практики	**Оцениваются:** полнота формирования компетенций при выполнении работ на практике; возможность использования, выполненных на практике работ, в качестве составной части ВКР.			
	У студента сформированы профессиональные компетенций и полученные на практике результаты будут полностью использованы в ВКР	**10-15**		
	У студента сформированы профессиональные компетенций не в полном объёме и полученные на практике результаты могут частично использованы в ВКР		**5-9**	
	У студента профессиональные компетенций сформированы слабо и полученные на практике результаты не могут быть использованы в ВКР			**1-4**

10.4 Типовые контрольные вопросы, необходимые для оценки результатов прохождения преддипломной практики

1. Принципы построения и особенности использования шифрованной файловой системы EFS.
2. Перечислите и охарактеризуйте основные встроенные механизмы защиты ОС.
3. Виды файловых систем. Контроль доступа к файлам.
4. Виртуальные частные сети (VPN): определение, назначение, способы организации.
5. Методы обеспечения защиты системы WWW и электронной почты.
6. Средства обеспечения защиты базовых протоколов и служб Internet семейства TCP/IP и службы поиска.
7. Классификация сетей, сравнительная характеристика различных типов сетей.
8. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности.
9. Понятие и виды защищаемой информации по законодательству РФ.
10. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
11. Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.
12. Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности.
13. Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации.
14. Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.
15. Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.
16. Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).
17. Основное содержание разработки Политики безопасности предприятия (организации).
18. Принципы, основные задачи и функции обеспечения информационной безопасности.
19. Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации.
20. Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.
21. Ответственность за нарушение законодательства в информационной сфере.
22. Основные мероприятия по защите информации при проведении совещаний и переговоров.
23. Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных).
24. Виды компьютерных преступлений. Классификация компьютерных злоумышленников.
25. Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП).
26. Раскрыть основной порядок проведения аттестации и контроля объектов информатизации.
27. Сформулировать основные правила безопасной работы в компьютерной системе.
28. Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД.
29. Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.
30. Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.

31. Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения.
32. Раскрыть понятие «компьютерный вирус». Привести виды компьютерных вирусов. Раскрыть жизненный цикл вирусов и механизмы сокрытия вредоносных программ.
33. Назначение и основные особенности применения системы защиты конфиденциальной информации «Aura».
34. Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.
35. Рассмотреть особенности разграничения доступа и аудита в СЗИ (на примере СЗИ «Аура»).
36. Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.
37. Раскрыть особенности организации технического противодействия лазерному подслушиванию.
38. Раскрыть особенности образования электромагнитных каналов утечки информации.
39. Раскрыть особенности образования и съема информации по электрическим каналам утечки информации.
40. Сформулировать основные особенности построения периметровой охраны особо важных объектов.

11. Особенности проведения практики

Подготовка студентов к преддипломной практике основана на реализации мероприятий организационного и методического характера, создающих основу для достижения заданных показателей качества практики в целом.

В ходе преддипломной практики студенты используют технологии:

- личностно-ориентированного обучения;
- информационные;
- проектного и проблемного обучения;
- инженерного поиска и оптимизации технических решений по последовательно применяемым критериям.

Практика студента должна проходить в одном из профилирующих подразделений организации, непосредственно связанным с защитой информационных ресурсов организации. С деятельностью других подразделений студент знакомится по мере выполнения программы практики с сохранением рабочего места в данном подразделении. Студентам следует особое внимание уделить изучению особенностей реализации комплексных систем защиты информации, программно-аппаратным средствам зашиты в автоматизированных системах, нормативным документам, регламентирующим построение, работу и мониторинг систем безопасности.

Она начинается в конце четвертого семестра и проявляется в виде регулярных встреч и бесед со студентами представителей деканата, кафедры, ответственной за организацию и проведение практики, и, в первую очередь, ответственного за организацию преддипломной практики от кафедры.

Инструктаж студентов является важнейшим мероприятием по управлению преддипломной практикой, от качества проведения, которого во многом зависит качество практики в целом, отношение студентов к практике в организациях, на предприятиях, учебная и производственная дисциплина студентов и т.д.

Инструктаж имеет целью:

- информировать студентов о сроках, целях и задачах практики;
- довести до студентов распределение фонда рабочего времени в период практики;
- информировать студентов о местах прохождения практики и о руководителях практики от университета;
- довести до сведения особенности прохождения практики в конкретной организации;

- сообщить требования по написанию отчета и срокам его сдачи;

- выдать студентам программу практики и индивидуальные задания на практику;

- напомнить студентам, какие документы они должны иметь при себе для трудоустройства на период практики в конкретной организации;

- в обязательном порядке, под роспись осветить вопросы соблюдения студентами правил техники безопасности и охраны труда (обеспечения безопасности жизнедеятельности) во время практики в конкретной организации, на предприятии;

Осветить вопросы режима работы организации, предприятия, правила внутреннего распорядка, этико-моральной дисциплины студентов во время практики.

Во избежание несчастных случаев на практике студенты должны хорошо знать и неукоснительно выполнять правила техники безопасности.

Перед убытием на практику кафедра (ответственный за организацию преддипломной практики) организует для студентов вводный инструктаж по охране труда и технике безопасности в период практики.

Студенты, не прошедшие вводный инструктаж по охране труда и технике безопасности, к прохождению практики не допускаются.

На базе практики соответствующими службами проводится вводный инструктаж и первичный инструктаж на рабочих местах. Особое внимание необходимо уделять следующим вопросам:

- правилам внутреннего распорядка и трудовой дисциплине;

- правилам, инструкциям и нормам по технике безопасности, промышленной санитарии, электробезопасности и пожарной безопасности;

- санитарно-гигиеническим мероприятиям, проводимым в цехе;

- порядку регистрации и учета несчастных случаев на предприятии;

- правам и обязанностям должностных лиц, отвечающих за технику безопасности и безопасность жизнедеятельности;

- приемам безопасной работы на технологическом оборудовании;

- защитным приспособлениям для глаз и рук, используемым при обработке металлов;

- охране окружающей среды и безопасности жизнедеятельности.

При переводе студентов на другое рабочее место службами предприятия проводится повторный инструктаж на новом рабочем месте.

В процессе контроля хода преддипломной практики осуществляется оперативное управление выполнением программы практики, графика ее прохождения и индивидуального задания. Со стороны вуза практику контролируют руководитель практики, заведующий кафедрой, представители деканата. Контролирующий должен принимать оперативные меры по устранению выявленных недостатков, а о серьезных недостатках, случаях травматизма немедленно докладывать руководству вуза и предприятия – базы практики.

Баланс времени практиканта определяется исходя из шестидневной рабочей недели и 8 часового рабочего дня.

12. Требования по проведению практики для инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

Форма проведения практики для обучающихся из числа лиц с ограниченными возможностями здоровья (инвалидностью) устанавливается с учетом индивидуальных психофизических особенностей в формах, адаптированных к ограничениям их здоровья и восприятия информации (устно, письменно на бумаге, письменно на компьютере и т.п.).

Выбор мест прохождения практик для инвалидов и лиц с ОВЗ производится с учетом требований их доступности для данных обучающихся и рекомендации медико-социальной экспертизы, а также индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда. При направлении инвалида и обучающегося с ОВЗ в организацию или предприятие для прохождения предусмотренной учебным планом практики Университет согласовывает с организацией (предприятием) условия и виды труда с уче-

том рекомендаций медико-социальной экспертизы и индивидуальной программы реабилитации инвалида. При необходимости для прохождения практик могут создаваться специальные рабочие места в соответствии с характером нарушений, а также с учетом профессионального вида деятельности и характера труда, выполняемых обучающимся-инвалидом трудовых функций.

Защита отчета по практике для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется с использованием средств общего и специального назначения. Перечень используемого материально-технического обеспечения:

- учебные аудитории, оборудованные компьютерами с выходом в интернет, видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном;
- библиотека, имеющая рабочие места для обучающихся, оборудованные доступом к базам данных и интернетом;
- компьютерные классы;
- аудитория Центра сопровождения обучающихся с инвалидностью с компьютером, оснащенная специализированным программным обеспечением для обучающихся с нарушениями зрения, устройствами для ввода и вывода голосовой информации.

Для лиц с нарушениями зрения материалы предоставляются:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

Защита отчета по практике для лиц с нарушениями зрения проводится в устной форме без предоставления обучающимся презентации. На время защиты в аудитории должна быть обеспечена полная тишина, продолжительность защиты увеличивается до 1 часа (при необходимости). Гарантируется допуск в аудиторию, где проходит защита отчета, собаки-проводника при наличии документа, подтверждающего ее специальное обучение, выданного по форме и в порядке, утвержденных приказом Министерства труда и социальной защиты Российской Федерации 21 июля 2015г., регистрационный номер 38115).

Для лиц с нарушениями слуха защита проводится без предоставления устного доклада. Вопросы комиссии и ответы на них представляются в письменной форме. В случае необходимости, вуз обеспечивает предоставление услуг сурдопереводчика.

Для обучающихся с нарушениями опорно-двигательного аппарата защита итогов практики проводится в аудитории, оборудованной в соответствии с требованиями доступности. Помещения, где могут находиться люди на креслах-колясках, должны размещаться на

уровне доступного входа или предусматривать пандусы, подъемные платформы для людей с ограниченными возможностями или лифты. В аудитории должно быть предусмотрено место для размещения обучающегося на коляске.

Дополнительные требования к материально-технической базе, необходимой для представления отчета по практике лицом с ограниченными возможностями здоровья, обучающийся должен предоставить на кафедру не позднее, чем за два месяца до проведения процедуры защиты.

Сведения о программе практики и ее согласовании

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

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

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

Председатель методической комиссии _____/Жестовский А.Г./

СОГЛАСОВАНО

Начальник отдела практики БГАРФ _____/Глущенко Е.И./