МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДЕНО
Ученым советом МГТУ им. Г.И. Носова
Протокол № 4 от « 26 » февраля 2020 г

Ректор МГТУ им. Г.И. Носова,
председатель ученого совета
_____ М.В. Чукин

МАТРИЦА ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ПО ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Специальность
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Направленность (специализация) программы
Обеспечение информационной безопасности распределенных информационных систем

Магнитогорск, 2020

ОП-АИБ-20-1,2

8.2 МАТРИЦА ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ		
ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции		
Знать	основные философские категории и специфику их понимания в различных исторических типах философии и авторских подходах; - основные направления философии и различия философских школ в контексте истории; - основные направления и проблематику современной философии;	Философия
Уметь	- раскрывать смысл выдвигаемых идей, корректно выражать и аргументировано обосновывать положения предметной области знания; - представлять рассматриваемые философские проблемы в развитии; - сравнивать различные философские концепции по конкретной проблеме; - уметь отметить практическую ценность определенных философских положений и выявить основания, на которых строится философская концепция или система;	
Владеть	- навыками работы с философскими источниками и критической литературой; - приемами поиска, систематизации и свободного изложения философского материала и методами сравнения философских идей, концепций и эпох; - способами обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации; - владеть навыками выражения и обоснования собственной позиции относительно современных социогуманитарных проблем и конкретных философских позиций	
Знать	-культурологические концепции и теории, формирующие представление о различных мировоззренческих позициях их авторов; -сущность понятия культурная картина мира, отражающего особенности мировоззрения личности; -причины формирования различных мировоззренческих позиций, основанных на философских знаниях представителей различных культурных систем	Культурология и межкультурное взаимодействие
Уметь	-выстраивать собственную мировоззренческую позицию на основе имеющихся культурно-философских знаний; -обосновывать собственную мировоззренческую позицию; -формировать новые взгляды и представления, основанные на существующих	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	мировоззренческих позициях представителей различных культурных систем	
Владеть	- методом критического анализа в области основ философских знаний с целью формирования собственной мировоззренческой позиции; - приемами убеждения в верности собственной мировоззренческой позиции; - навыком отбора значимых философских знаний для формирования мировоззренческой позиции	
ОК-2: способностью использовать основы экономических знаний в различных сферах деятельности		
Знать	- основные термины, определения, экономические законы и взаимозависимости на уровне экономики в целом и на уровне отдельного предприятия; - методы исследования экономических отношений на уровне экономики в целом и на уровне отдельного предприятия; - методики расчета важнейших экономических показателей и коэффициентов на уровне экономики в целом и на уровне отдельного предприятия; - теоретические принципы выработки экономической политики на уровне государства и на уровне отдельного предприятия.	Экономика
Уметь	- ориентироваться в типовых экономических ситуациях, основных вопросах экономической политики; - использовать элементы экономического анализа в своей профессиональной деятельности; - рационально организовать свое экономическое поведение в качестве агента рыночных отношений, - анализировать и объективно оценивать процессы и явления, осуществляющиеся в рамках национальной экономики в целом и отдельного предприятия в частности. - ориентироваться в учебной, справочной и научной литературе.	
Владеть	- методами и приемами анализа экономических явлений и процессов на уровне экономики в целом и на уровне отдельного предприятия; - практическими навыками использования экономических знаний на других дисциплинах, на занятиях в аудитории и на практике; - на основании теоретических знаний принимать решения на уровне экономики в целом и на уровне отдельного предприятия; - самостоятельно приобретать, усваивать и применять экономические знания, наблюдать,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	анализировать и объяснять экономические явления, события, ситуации.	
Знать	- систему финансирования инновационной деятельности в различных сферах жизнедеятельности; - принципы, формы и методы финансирования научно-технической продукции; - средства и методы стимулирования сбыта продукции.	Продвижение научной продукции
Уметь	- анализировать экономическую и научную литературу; - анализировать рынок научно-технической продукции; - рассчитывать экономические показатели структурного подразделения организации; - анализировать существующие и потенциальные запросы потребителей, возможностей создания ценностей для потребителя с учетом особенностей жизненного цикла продукции и технологий; - выделять основные этапы продвижения научного товара и пути его совершенствования в условиях Российского рынка научной продукции; - определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов.	
Владеть	- способами оценивания значимости и практической пригодности инновационной продукции; - методами стимулирования сбыта продукции; - расчетом цен инновационного продукта; - современными методиками расчета и анализа показателей и индикаторов, характеризующие инновационную деятельность предприятия и возможности реализации инновационного проекта.	
Знать	основные определения и понятия из области инновационной экономики и технологического предпринимательства; специфику предпринимательской деятельности.	Технологическое предпринимательство
Уметь	Выделять объекты предпринимательской деятельности; обсуждать способы эффективного решения задач; распознавать эффективное решение от неэффективного; выявлять и строить типичные модели инновационных задач;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	корректно выражать и аргументировано обосновывать экономические положения, связанные с предпринимательской деятельностью	
Владеть	основами применения экономических знаний в сфере предпринимательской деятельности, в том числе алгоритмами оценки эффективности предпринимательской деятельности	
ОК – 3 – способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма		
Знать	-Основные проблемы, периоды, тенденции и особенности исторического процесса, -Осознавать место истории России во всемирно-историческом процессе	История
Уметь	выражать и обосновывать свою позицию по вопросам, касающимся ценностного отношения к историческому прошлому.	
Владеть	Навыками межличностной и межкультурной коммуникации, основанные на уважении к историческому наследию и культурным традициям	
Знать:	Процесс историко-культурного развития человека и человечества; всемирную и отечественную историю и культуру; особенности национальных традиций, текстов; движущие силы и закономерности исторического процесса; место человека в историческом процессе; политическую организацию общества.	Физическая культура и спорт
Уметь:	Определять ценность того или иного исторического или культурного факта или явления; уметь соотносить факты и явления с исторической эпохой и принадлежностью к культурной традиции; проявлять и транслировать уважительное и бережное отношение к историческому наследию и культурным традициям; анализировать многообразие культур и цивилизаций; оценивать роль цивилизаций в их взаимодействии.	
Владеть:	Навыками исторического, историко-типологического, сравнительно -типологического анализа для определения места профессиональной деятельности в культурно-исторической парадигме; навыками бережного отношения к культурному наследию и человеку; информацией о движущих силах исторического процесса; приемами анализа сложных социальных проблем в контексте событий мировой истории и современного социума.	
ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности		
Знать	основные правовые понятия; основные источники права; принципы применения юридической ответственности	Правоведение

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	ориентироваться в системе законодательства; определять соотношение юридического содержания норм с реальными событиями общественной жизни; разрабатывать документы правового характера; приобретать знания в области права; корректно выражать, аргументировано обосновывать свою юридическую позицию	
Владеть	практическими навыками анализа и разрешения юридических ситуаций; практическими навыками совершения юридических действий в соответствии с законом; навыками составления претензий, заявлений, жалоб по факту неисполнения или ненадлежащего исполнения прав; способами совершенствования правовых знаний и умений путем использования возможностей информационной среды	
Знать	-основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Организационное и правовое обеспечение информационной безопасности
Уметь	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности - владения юридической терминологией; -навыками работы с правовыми актами; навыками реализации правовых норм; навыками принятия необходимых мер правового регулирования и (или) защиты интересов субъектов правовых отношений	
Владеть	навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике	
Знать	- основы законодательства Российской Федерации; - нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации;	Управление информационной

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- правовые основы организации защиты государственной тайны и конфиденциальной информации; - меры правовой и дисциплинарной ответственности за разглашение защищаемой информации	безопасностью
Уметь	- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей; - предпринимать необходимые меры по восстановлению нарушенных прав.	
Владеть	- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.	
Знать	- основные виды охранных документов интеллектуальной собственности; - ключевые этапы и правила государственной системы регистрации результатов научной деятельности; - формы государственной поддержки инновационной деятельности в России.	Продвижение научной продукции
Уметь	- анализировать социально-политическую и научную литературу; - оформлять документацию; - использовать основные правовые знания при закреплении основных результатов экспериментальной и исследовательской работы; - составлять пакет документов для регистрации изобретения или полезной модели; - составлять пакет документов для регистрации программы ЭВМ.	
Владеть	- вопросами правового регулирования деятельности предприятия; - знаниями о научно-технической политики России; - навыками составления конкурсной документации.	
Знать	законодательную основу в области предпринимательской деятельности	Технологическое предпринимательство
Уметь	использовать правовые знания в сфере предпринимательской деятельности	
Владеть	навыками использования законодательной базы при организации предпринимательской деятельности	
ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		
Знать	политику государства в области обеспечения информационной безопасности национальные, межгосударственные и международные стандарты в области защиты	Введение в специальность

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информации руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации современное состояние рынка труда в области обеспечения информационной безопасности профессиональный стандарт «Специалист по защите информации в автоматизированных системах» перечень сведений, составляющих государственную тайну трудовое законодательство РФ	
Уметь	применять действующую нормативную базу в области обеспечения безопасности информации определять источники и причины возникновения инцидентов информационной безопасности оценивать последствия выявленных инцидентов оценивать информационные риски в автоматизированных системах	
Владеть	навыками определения структуры системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы	
Знать	- политику государства в области обеспечения информационной безопасности - национальные, межгосударственные и международные стандарты в области защиты информации - современное состояние рынка труда в области обеспечения информационной безопасности - профессиональный стандарт «Специалист по защите информации в автоматизированных системах» - трудовое законодательство РФ	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	- анализировать информацию по вопросам национальной и информационной безопасности государства; - соблюдать нормы профессиональной этики	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	- профессиональной терминологией в области информационной безопасности; - практическими навыками соблюдения норм профессиональной этики	
Знать	- основные профессиональные задачи специалиста по информационной безопасности; - перечень инструкций для информирование персонала об угрозах безопасности информации и о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации; - основы кибербезопасности;	Основы безопасности цифрового общества
Уметь	- критически оценивать информацию, полученную в цифровой среде; - оценить достоверность информации, полученной в цифровой среде; - строить логические умозаключения на основании поступающих информации и данных;	
Владеть	- критическим мышлением для анализа информации в цифровой среде; - основами профессиональной деятельности в сфере цифровой экономики в условиях нарастающих угроз безопасности информации;	
ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различи		
Знать	– суть культурных отношений в обществе, место человека в культурном процессе и жизни общества; – содержание актуальных культурных и общественно значимых проблем современности; – методы и приемы социокультурного анализа проблем современности, основные закономерности культурно-исторического процесса.	Культурология и межкультурное взаимодействие
Уметь	– анализировать и оценивать социокультурную ситуацию; – объективно оценивать многообразные культурные процессы и явления; – планировать и осуществлять свою деятельность с позиций сотрудничества, с учетом Результатов анализа культурной информации.	
Владеть	– навыками коммуникаций в профессиональной сфере, критики и самокритики, терпимостью; – навыками культурного сотрудничества, ведения переговоров и разрешения конфликтов; – навыками толерантного восприятия социальных и культурных различий.	
Знать	принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия	Технология командообразования и

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	находить организационно - управленческие решения в нестандартных ситуациях	саморазвития
Владеть	умением находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность	
Знать	– содержание актуальных культурных и общественно значимых проблем современности; – методы и приемы социокультурного анализа проблем современности, основные закономерности культурно-исторического процесса.	Производственная-преддипломная практика
Уметь	– анализировать и оценивать социокультурную ситуацию; – планировать и осуществлять свою деятельность с позиций сотрудничества, с учетом результатов анализа культурной информации.	
Владеть	– навыками коммуникаций в профессиональной сфере, критики и самокритики, терпимостью; – навыками культурного сотрудничества, ведения переговоров и разрешения конфликтов; – навыками толерантного восприятия социальных и культурных различий.	
ОК-7 способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности		
Знать	лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского минимума и потенциального словаря, включая термины профилирующей специальности; - определенные приемы, позволяющие совершать познавательную и коммуникативную деятельность; - структурные типы простого предложения, грамматические формы и конструкции; порядок слов простого предложения; - виды письменных и устных высказываний в различных коммуникативных ситуациях; - разговорные формулы этикета профессионального общения, приемы структурирования научногодискуса.	Иностранный язык
Уметь	- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного языка; - работать с оригинальной литературой научного характера, сопоставлять и определять/	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	выбирать пути и способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций); - применять полученные знания для преодоления трудностей при переводе с учетом вида перевода, его целей и условийосуществления.	
Владеть	- подготовленной, а также неподготовленной монологической и диалогической речью в пределах изученного языкового материала и в соответствии с избранной специальностью; - терминологией по специальности, а также дискурсивными, лексико-фразеологическими, грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной профессиональной деятельности; - правильно оперировать языковыми средствами английского языка в ситуациях устного общения; - всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое); - письмом в пределах изученного материала (250-300 слов).	
Знать	– структуру и содержание межкультурного взаимодействия; – суть ценностно-смысловых отношений в межличностной коммуникации; – материальную и духовную роль культуры в развитии современного общества; – движущие силы и закономерности культурного процесса, многоварантность культурного процесса.	Культурология и межкультурное взаимодействие
Уметь	– общаться с представителями других культур, используя приемы межкультурного взаимодействия; – решать задачи межличностного и межкультурного взаимодействия в профессиональной деятельности; – анализировать проблемы культурных процессов; – применять понятийно-категориальный аппарат, основные законы культурологии как гуманитарной науки в профессиональной деятельности; – анализировать и оценивать культурные процессы и явления, планировать и осуществлять свою деятельность с учетом результатов этого анализа.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	– навыками межкультурного взаимодействия; – критического восприятия культурно значимой информации; – навыками социокультурного анализа современной действительности; – навыками социального взаимодействия, сотрудничества впозиций расовой, национальной, религиозной терпимости.	
Знать	– понятие и содержание управленческой деятельности	Основы управленческой деятельности
Уметь	– анализировать внешнюю и внутреннюю среду организации как объекта управленческой деятельности	
Владеть	– основными навыками управленческой деятельности: планирования, организации, мотивации, контроля и коммуникаций	
Знать	- лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского минимума и потенциального словаря, включая термины профилирующей специальности; - определенные приемы, позволяющие совершать познавательную и коммуникативную деятельность; - структурные типы простого предложения, грамматические формы и конструкции; порядок слов простого предложения; - виды письменных и устных высказываний в различных коммуникативных ситуациях; - разговорные формулы этикета профессионального общения, приемы структурирования научного дискурса.	Иностранный язык в профессиональной деятельности
Уметь	- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного языка; - работать с оригинальной литературой научного характера, сопоставлять и определять/ выбирать пути и способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций); - применять полученные знания для преодоления трудностей при переводе с учетом вида	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	перевода, его целей и условийосуществления.	
Владеть	- подготовленной, а также неподготовленной монологической и диалогической речью в пределах изученного языкового материала и в соответствии с избранной специальностью; - терминологией по специальности, а также дискурсивными, лексико-фразеологическими, грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной профессиональной деятельности; - правильно оперировать языковыми средствами английского языка в ситуациях устного общения; - всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое); - письмом в пределах изученного материала (250-300 слов).	
ОК-8: способностью к самоорганизации и самообразованию		
Знать	способы самоорганизации и развития своего интеллектуального, культурного, духовного, нравственного, физического и профессионального уровня	Технология командообразования и саморазвития
Уметь	находить недостатки в своем общекультурном и профессиональном уровня развития и стремиться их устранить; планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения осуществления деятельности	
Владеть	технологиями организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности	
Знать	- порядок и особенности выполнения научно-исследовательских работ по государственным контрактам; - отличительныепризнакиинновационнойпродукции.	Продвижение научной продукции
Уметь	- приобретать знания в области продвижения научной продукции; - определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	- классификацией научно-технической продукции, профессиональным языком в области продвижения научной продукции; - практическими навыками оценки качества для научно-технической продукции, навыками составления конкурсной документации.	
Знать	Комплекс необходимых действий процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей предпринимательской деятельности	Технологическое предпринимательство
Уметь	планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения личных целей при осуществлении предпринимательской деятельности.	
Владеть	владеть приемами самоорганизации и способами самообразования при осуществлении предпринимательской деятельности	
ОК-9 — способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности		
Знать	Основные средства и методы физического воспитания, основные методики планирования самостоятельных занятий по физической культуре с учетом анатомо-физиологических особенностей организма и организации ЗОЖ, с целью укрепления здоровья, повышения уровня физической подготовленности.	Физическая культура и спорт
Уметь	Применять полученные теоретические знания по организации и планированию занятий по физической культуре анатомо- физиологических особенностей организма. Применять теоретические знания по организации самостоятельных занятий с учетом собственного уровня физического развития и физической подготовленности. Использовать тесты для определения физической подготовленности с целью организации самостоятельных занятий по определенному виду спорта с оздоровительной направленностью, для подготовки к профессиональной деятельности.	
Владеть	Средствами и методами физического воспитания. Методиками организации и планирования самостоятельных занятий по физической культуре. Методиками организации физкультурных и спортивных занятий с учетом уровня физической подготовленности и профессиональной деятельности, навыками и умениями самоконтроля	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Знать	основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; знание технических приемов и двигательных действий базовых видов спорта; современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	Элективные курсы по физической культуре и спорту
Уметь	использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности; использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности; анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств; самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике; навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности; практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; техническими приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности; навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	
Знать:	основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; знание технических приемов и двигательных действий базовых видов спорта; современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	Адаптивные курсы по физической культуре и спорту

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь:	использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике; выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности; использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности; анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью; анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств; самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	
Владеть:	практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике; навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности; практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга; техническими приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности; навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	связанных с учебной и производственной деятельностью; основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств; навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).	
ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ		
ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач		
Знать	О современных научных представлениях окружающего мира, о новых открытия в физике и естествознании. Основные положения аксиоматических физических теорий (классической механики, релятивистской механики, статистической физики, термодинамики, теории электромагнетизма, классической квантовой механики) включающие: 1) описание состояния системы; 2) уравнения изменения состояния системы; 3) математический аппарат; 4) границы применимости данной теории. Основные структурные элементы процесса физического измерения: объект - его модель; средство измерения - его модель; результат измерения - его модель и т.д. Погрешности измерения. Методы и подходы к теоретическому и экспериментальному исследованию, применяемые в физике и распространяющиеся на другие области знаний Единицы физических величин в СИ	Физика
Уметь	распознавать эффективное решение от неэффективного (бритва Аккамы); объяснять (выявлять и строить) типичные физические модели для описания реальных процессов, выбирать методы исследования по характеристикам физических приборов; применять физические законы и физико-математический аппарат в профессиональной деятельности; использовать их на междисциплинарном уровне; приобретать знания физики для решения инженерных задач; аргументировано обосновывать выводы эксперимента. **корректно планировать план физического эксперимента**	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	различать четыре вида измерения (прямые, косвенные, совокупные и совместные) и уметь осуществлять метрологическую обработку результатов физического эксперимента этих видов измерения.	
Владеть	навыками решения физических задач; навыками работы с широким кругом физических приборов и оборудования; способами использования физических законов при решении инженерных задач; методами проведения физических измерений, расчета величин, анализа полученных данных и навыками планирования исследовательского процесса; навыками и методиками обобщения результатов экспериментальной деятельности; способами оценивания значимости и практической пригодности полученных результатов; профессиональным языком в области физики и информатики; способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды. инженерными навыками использования программных средств для физико-математических моделей в конкретной предметной области	
Знать	Математические методы расчёта электрических цепей, теорию четырёхполюсников, Фурье преобразование и преобразования Лапласса, основы цифровой обработки сигналов	Электроника и схемотехника
Уметь	Рассчитывать электрические цепи, рассчитывать параметры четырёхполюсников, рассчитывать параметры и характеристики фильтров и усилителей сигналов, рассчитывать процессы в длинных линиях, рассчитывать схемы на операционных усилителях, рассчитывать цифровые схемы	
Владеть	Навыками проектирования схем аналоговой и цифровой электроники для обработки информации	
Знать	Физические основы функционирования систем обработки и передачи информации. Основные физические явления и законы, используемые при построении средств защиты информации от утечки по техническим каналам. Техническиеканалыутечкиинформации	Техническая защита информации
Уметь	Применять соответствующий математический аппарат при проведении расчетов защищенности информации Контролировать безотказное функционирование технических средств защиты информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Заменять отказавшие технические средства защиты информации	
Владеть	Навыками работы с нормативными правовыми актами в области технической защиты информации. Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.	
Знать	– физическую сущность процессов, происходящих в системах передачи информации в целом; – физическую сущность процессов, происходящих в отдельных узлах систем передачи информации; – физическую сущность процессов, происходящих в элементах узлов систем передачи информации.	Основы радиотехники
Уметь	– разрабатывать модели процессов, происходящих в системах передачи информации в целом; – разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации; – разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.	
Владеть	– математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом; – математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации; – математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.	
Знать	– физическую сущность процессов, происходящих в системах передачи информации в целом; – физическую сущность процессов, происходящих в отдельных узлах систем передачи информации; – физическую сущность процессов, происходящих в элементах узлов систем передачи информации.	Физические основы передачи информации
Уметь	– разрабатывать модели процессов, происходящих в системах передачи информации в целом; – разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации; – разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	– математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом; – математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации; – математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.	
Знать	– Физические основы функционирования систем обработки и передачи информации. – Принципы построения средств защиты информации от утечки по техническим каналам. – Технические каналы утечки информации. – Технические средства контроля эффективности мер защиты информации.	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	– Контролировать безотказное функционирование технических средств защиты информации. – Восстанавливать отказавшие технические средства защиты информации. – Заменять отказавшие технические средства защиты информации.	
Владеть	– Навыками работы с нормативными правовыми актами в области технической защиты информации. – Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.	
ОПК-2 – способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники		
Знать	- основные понятия линейной алгебры и аналитической геометрии - возможности координатного метода для исследования различных геометрических объектов - аналитические способы описания алгебраических структур и геометрических объектов	Алгебра и геометрия
Уметь	- сопоставлять реальную задачу с определенной областью математических знаний, - распознавать возможность аналитического решения задачи, - самостоятельно разрабатывать алгоритм решения задачи, - применять типичные математические модели линейной алгебры и аналитической геометрии в профессиональной деятельности;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- корректно обосновывать необходимость предложенного метода решения задачи; - формализовать задачу и находить ее решение, используя свойства математических объектов алгебры и геометрии; - интерпретировать формально (математически) полученный результат	
Владеть	- методами работы с алгебраическими и геометрическими объектами, - методами построения и изучения математических моделей конкретных явлений и процессов для решения расчетных и исследовательских задач; - практическими навыками доказательства суждений; - умением теоретически обосновывать выводы; - математическими методами описания реальных процессов в профессиональной деятельности.	
Знать	основные положения теории пределов функции; - основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных, - основные понятия теории функций комплексной переменной; - основные методы решения обыкновенных дифференциальных уравнений - основные понятия теории числовых и функциональных рядов	Математический анализ
Уметь	- решать задачи по изучаемым теоретически разделам; - обсуждать способы эффективного решения дифференциальных уравнений и их систем; - определять эффективность решения задачи, полученного с помощью численных методов; - распознавать эффективные результаты обработки экспериментальных данных от неэффективных	
Владеть	- практическими навыками использования математических понятий и методов (изучаемых разделов математики) при решении прикладных задач; - способами оценивания значимости и практической пригодности полученных результатов; - навыками построения и решения математических моделей прикладных задач	
Знать	Основные методы исследований, используемых в теории вероятностей и математической статистике Основные законы, правила и определения процессов	Теория вероятностей, математическая статистика
Уметь	Выделять главное, существенное при решении поставленных задач Обсуждать способы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	эффективного решения поставленных задач Распознавать эффективное решение от неэффективного Объяснять (выявлять и строить) типичные модели поставленных задач	
Владеть	Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат теории вероятностей, математической статистики, в том числе с использованием вычислительной техники.	
Знать	Общие положения теории оптимизации; – Логическую, функциональную и структурную схему персонального компьютера, устройства организующие работу вычислительных систем; – Способы применения теоретических положений и методов теории оптимизации для постановки и решении профессиональных задач.	Основы теории оптимизации
Уметь	Проводить теоретические исследования применения общих положений и методов теории оптимизации; – Определять возможности применения теоретических положений и методов теории оптимизации для постановки и решения конкретных прикладных задач; – Эффективно использовать и оптимизировать свою работу за счет применения общих положений и методов теории оптимизации	
Владеть	Приемами использования соответствующего математического аппарата при решении профессиональных задач; – Приемами сбора и анализ исходных данных для последующей обработки соответствующим математическим аппаратом; – Навыками повышения эффективности работы за счет применения общих положений и методов теории оптимизации	
Знать	теоретические основы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов; – основные принципы и схемы автоматического управления; – основные типы систем автоматического управления, их математическое описание и основные задачи исследования систем с распределенными параметрами	Математическое моделирование распределенных систем
Уметь	применять математические методы для анализа общих свойств линейных распределенных систем; – применять методы расчета и исследования систем автоматического управления объектами с	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	распределенными параметрами; – применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований.	
Владеть	методами преобразования структурных схем распределенных систем управления; – методами преобразования структурных схем распределенных систем управления; – методами и навыками преобразования структурных схем распределенных систем управления.	
Знать	Основные идеи комбинаторики, понятия теории множеств, булевой алгебры, теории конечных автоматов и графов	Дискретная математика
Уметь	Применять методы дискретной математики для решения практических задач Выбирать и применять методы дискретной математики и средства вычислительной техники для решения практических задач	
Владеть	Навыками применения математического аппарата дискретной математики для формализации, анализа и выработки решения профессиональных задач с использованием вычислительной техники	
Знать	способы представления и обработки информации с помощью алгоритмов (в том числе, реализованных на современных языках логического программирования), методологию построения математических алгоритмов, методы математического моделирования	Математическая логика и теория алгоритмов
Уметь:	корректно применять аппарат математической логики для формализации и решения задач в сфере профессиональной деятельности строить математические алгоритмы, используемые при решении задач в конкретных областях знаний. формулировать полученные результаты в терминах предметной области изучаемого объекта	
Владеть	основными методами математического и алгоритмического моделирования; навыками применения вычислительных методов для решения задач профессиональной деятельности навыками построения эффективных алгоритмов с точки зрения теории вычислимости	
Знать	- основы теории информации; - способы измерения количественных характеристик информации; - способы измерения качественных характеристик информационных систем;	Теория информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- основные методы эффективного кодирования; - основные методы помехозащищенного кодирования;	
Уметь:	применять основные постулаты теории информации; - применять современные методы теории информации для решения практических задач; - применять знания, полученные в ходе освоения дисциплины при работе над междисциплинарными и инновационными проектами; - применять методы эффективного кодирования; - применять методы помехозащищенного кодирования;	
Владеть	профессиональным языком предметной области знания; - современными методиками кодирования; - методиками оценки эффективности алгоритмов сжатия; - методиками оценки эффективности алгоритмов помехоустойчивого кодирования;	
Знать:	Классификацию современных компьютерных систем; ─ Классификацию системного и прикладного программного обеспечения; ─ Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.	Информатика
Уметь:	Пользоваться расчетными формулами, таблицами, компьютерными программами при решении профессиональных задач; ─ Применять офисные приложения (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов) в профессиональной деятельности; ─ Эффективно использовать современные компьютерные технологии для решения профессиональных задач.	
Владеть:	Навыками работы с реляционными системами управления базами данных при решении профессиональных задач; ─ Навыками проектирования и реализации алгоритмов для решения профессиональных задач; ─ Навыками создания, отладки и выполнения программ интегрированных сред разработки офисных приложений.	
Знать:	Основные методы исследования операций и теории игр Определения основных понятий, называет их структурные характеристики Основные законы, правила и определения процессов	Исследование операций и теория игр
Уметь:	Выделять главное, существенное при решении поставленных задач Обсуждать способы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	эффективного решения поставленных задач Распознавать эффективное решение от неэффективного	
Владеть:	Методами исследования операций и теории игр при разработке и исследования моделей информационно- технологических ресурсов Методиками обобщения результатов решения, экспериментальной деятельности	
Знать:	-Основы применения теории графов при решении задач на ЭВМ Способы классификации и виды графов направления развития теории графов -Новые технологии применения теории графов в моделировании предметных областей -связи теории графов с другими предметами, различные информационные технологии, используемые в теории графов	Теория графов и ее приложения
Уметь:	-Применять методы теории графов при решении задач на ЭВМ -Самостоятельно приобретать знания и применять теорию графов при решении задач на ЭВМ -Классифицировать задачи теории графов по степени сложности и применять соответствующие алгоритмы для решения задач	
Владеть:	-Методологическими основами формирования изучения графов и их свойств при исследовании и построении систем -Приемами исследования проблем области теории графов, возникающих в различных сферах человеческой деятельности -Навыками разработки и реализации наилучшего решения для поставленной задачи -Навыками решения оптимизационных задач теории графов и задач сетевого планирования	
Знать:	математический аппарат теории информации, теории алгоритмов • процессы генерации простых чисел для систем ассиметричного шифрования • процессы постановки и верификации ЭЦП • математический аппарат шифра скользящей перестановки • принцип работы сети Фейстеля как базовым преобразованием симметричных блочных криптосистем	Криптографические методы защиты информации
Уметь:	корректно применять при решении профессиональных задач математический аппарат теории алгоритмов, теории информации, в том числе с использованием вычислительной техники • реализовывать методы генерации простых чисел средствами вычислительной техники • проводить дешифрование шифра простой перестановки при помощи метода биграмм	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть:	навыками использованием вычислительной техники для реализации криптографических алгоритмов	
ОПК-3 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности.		
Знать	Общие принципы построения современных языков программирования высокого уровня. Общие принципы использования современных языков программирования высокого уровня. Язык программирования высокого уровня (объектно- ориентированное программирование).	Языки программирования
Уметь	Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования. Проводить комплексное тестирование и отладку программных систем. Работать с интегрированной средой разработки программного обеспечения. Использовать шаблоны классов и средства макрообработки. Использовать динамически подключаемые библиотеки. Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования.	
Владеть	Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. Навыками работы с интегрированной средой разработки программного обеспечения. Навыками проектирования программного обеспечения с использованием средств автоматизации.	
Знать	Язык программирования высокого уровня (объектно- ориентированное программирование); Современные технологии и методы программирования; Показатели качества программного обеспечения; Методологии и методы проектирования программного обеспечения; Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; Принципы организации документирования разработки,процесса сопровождения программного	Технологии и методы программирования

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	обеспечения.	
Уметь	Работать с интегрированной средой разработки программного обеспечения; Использовать динамически подключаемые библиотеки; Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; Использовать шаблоны классов и средства макрообработки; Проводить комплексное тестирование и отладку программных систем; Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; Проводить выбор эффективных способов реализации профессиональных задач; Планировать разработку сложного программного обеспечения; Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; автоматизированных систем	
Владеть	Основными навыками проектирования программного обеспечения с использованием средств автоматизации. Навыками программирования различными стилями. Навыками разработки программной документации. Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования	
Знать	Виды аутентификации и принципы, на которых они основаны. Принципы программирования различных видов карт и ключей доступа. Типы атак на системы данных, использующих различные виды аутентификации	Безопасность систем баз данных
Уметь	Настраивать систему организации и контроля доступа различного вида. Анализировать и находить решения по защите от атак на системы данных, использующих различные виды аутентификации. Устанавливатьсредствазащиты БД.	
Владеть	Навыками настройки и администрирования средств защиты БД. Навыками разработки системы защиты с учетом особенностей защиты информации,	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	обрабатываемой в СУБД. Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.	
Знать	Основные принципы организации программных и программно- аппаратных СЗИ. Основные подходы создания программных и программно- аппаратных СЗИ. Основные подходы и способы реализации СКЗИ.	Информационная безопасность распределенных информационных систем
Уметь	Проводить комплексное тестирование и отладку программных и программно-аппаратных СЗИ. Администрировать программные и программно-аппаратные СЗИ. Проводить комплексное тестирование и отладку СКЗИ. Администрировать СКЗИ.	
Владеть	Навыками комплексного тестирования и отладки программных и программно-аппаратных систем защиты информации. Навыками администрирования программных и программно-аппаратных СЗИ. Навыками комплексного тестирования и отладки СКЗИ. Навыкамиадминистрирования СКЗИ.	
Знать	способы организации обмена данными по схеме «peer-to-peer»; - способы организации обмена данными при помощи технологии Socket - базовый синтаксис C#; - базовый функционал LabVIEW; - способы обработки ошибок; -способы организации многопоточности;	Технология построения защищенных распределенных приложений
Уметь	применять язык программирования C# для построения консольных клиент/серверных приложений для однократной передачи данных; - применять язык программирования LabVIEW для построения простейших клиент/серверных приложений для однократной передачи данных; - согласовывать формат передаваемых данных и логику обмена информацией.	
Владеть	- навыками разработки приложений на языке C# с применением многопоточности; - навыками разработки приложений на языке LabVIEW с применением многопоточности	
Знать	средства моделирования угроз информационной безопасности	Моделирование угроз информационной
Уметь	применять языки, системы и инструментальные средства программирования для	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	моделирования угроз информационной безопасности	безопасности
Владеть	навыками применения инструментальных средств программирования для моделирования угроз	
Знать	– язык программирования высокого уровня (объектно-ориентированное программирование); – современные технологии и методы программирования; – показатели качества программного обеспечения; – методологии и методы проектирования программного обеспечения; методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; – показатели качества программного обеспечения; принципы организации документирования разработки, процесса сопровождения программного обеспечения	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	– работать с интегрированной средой разработки программного обеспечения; – проводить комплексное тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; – проводить выбор эффективных способов реализации профессиональных задач; планировать разработку сложного программного обеспечения; – формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; автоматизированных систем;	
Владеть	– основными навыками проектирования программного обеспечения с использованием средств автоматизации; навыками и различными стилями программирования; – навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов; – навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования	
Знать	– Язык программирования высокого уровня (объектно-ориентированное программирование); – Современные технологии и методы программирования; – Показатели качества программного обеспечения; – Методологии и методы проектирования программного обеспечения;	Производственная-практика по получению профессиональных умений и опыта

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; – Принципы организации документирования разработки,процесса сопровождения программного обеспечения.	профессиональной деятельности
Уметь	– Работать с интегрированной средой разработки программного обеспечения; – Использовать динамически подключаемые библиотеки; – Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; – Использовать шаблоны классов и средства макрообработки; – Проводить комплексное тестирование и отладку программных систем; – Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; – Проводить выбор эффективных способов реализации профессиональных задач; – Планировать разработку сложного программного обеспечения; – Формировать требования и разрабатывать внешние спецификациидля разрабатываемого программного обеспечения; автоматизированных систем;	
Владеть	– Основными навыками проектирования программного обеспечения с использованием средств автоматизации. – Навыками программирования различными стилями. – Навыками разработки программной документации. – Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. – Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.	
Знать	– Язык программирования высокого уровня (объектно-ориентированное программирование); – Современные технологии и методы программирования; – Показатели качества программного обеспечения; – Методологии и методы проектирования программного обеспечения;	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; – Принципы организации документирования разработки,процесса сопровождения программного обеспечения.	
Уметь	– Работать с интегрированной средой разработки программного обеспечения; – Использовать динамически подключаемые библиотеки; – Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; – Использовать шаблоны классов и средства макрообработки; – Проводить комплексное тестирование и отладку программных систем; – Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; – Проводить выбор эффективных способов реализации профессиональных задач; – Планировать разработку сложного программного обеспечения; – Формировать требования и разрабатывать внешние спецификациидля разрабатываемого программного обеспечения; автоматизированных систем;	
Владеть	– Основными навыками проектирования программного обеспечения с использованием средств автоматизации. – Навыками программирования различными стилями. – Навыками разработки программной документации. – Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов. – Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.	
ОПК-4 - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах.		
Знать	─ Основные понятия информатики; ─ Основные способы хранения, обработки и передачи информации; ─ Основы технологии поиска в современных информационно- поисковых системах;	Информатика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	─ Значение информации в развитии современного общества	
Уметь	Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет; ─ Применять функции офисных приложений для организации поиска информации по заданным критериям; ─ Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач.	
Владеть	Навыками использования современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах при решении профессиональных задач; ─ Навыками построения запросов для организации поиска информации в компьютерных системах, сетях, библиотечных фондах	
Знать	– Основные понятия информатики; – Основные способы хранения и обработки информации; – Значение информации в развитии современного общества.	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь	– Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет; – Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет и библиотечными фондами по профилю деятельности; – Эффективно использовать и оптимизировать свою работу для обмена данными, с использованием глобальной информационной сети Интернет и библиотечными фондами.	
Владеть	– Представлением о возможности использования информационных технологий для решения профессиональных задач; – Способами использования информационных технологий для решения профессиональных задач; – Способами повышения эффективности использования информационных технологий для решения профессиональных задач.	
Знать	– основные направления развития, значение Big Data и их роль в современном обществе; – основные возможности ИКТ для поиска Big Data из различных источников	Основы Data инжиниринга

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информации.	
Уметь	– организовывать поиск Big Data в компьютерных системах, сетях и библиотечных фондах; – автоматизировать работу с большими массивами данных, получать данные из внешних источников.	
Владеть	– методами поиска, хранения и обработки Big Data из различных источников баз данных, библиотечных фондов; – методами представления Big Data с использованием информационных, компьютерных и сетевых технологий.	
ОПК-5: способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами		
Знать	- основные определения и понятия инженерной графики; - основные правила выполнения чертежей; - основные положения ЕСКД; - нормативные и руководящие материалы, касающиеся выполняемых типов чертежей	Инженерная графика
Уметь	- обсуждать способы эффективного решения задач (2D или 3D построения); - объяснять (выявлять и строить) типичные модели задач, чертежей и 3D моделей; - применять знания чтения и построения чертежей в профессиональной деятельности; - использовать знания чтения и построения чертежей и 3D моделей на междисциплинарном уровне	
Владеть	- практическими навыками использования элементов дисциплины для решения задач на других дисциплинах, на занятиях в аудитории и на производственной практике; - методами использования программных средств для решения практических задач; - основными методами решения задач в области инженерной графики; - возможностью междисциплинарного применения полученных знаний; - основными методами исследования в области инженерной и компьютерной графики, практическими умениями и навыками их использования	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении,	Информационная безопасность

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	организации. Подходы создания междисциплинарных и инновационных проектов.	распределенных информационных систем
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах	
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов.	
Знать	- средства и методы стимулирования сбыта продукции. Виды охранных документов интеллектуальной собственности; - основные шаги и правила государственной системы регистрации результатов научной деятельности.	Продвижение научной продукции
Уметь	- составлять пакет документов для регистрации программы ЭВМ; - составлять пакет документов для регистрации изобретения или полезной модели.	
Владеть	- способами анализа патентной документации и проведения патентного поиска; - способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды.	
Знать	Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации. Подходы создания междисциплинарных и инновационных проектов.	Научно-исследовательская работа
Уметь	Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации. Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации. Принимать участие в междисциплинарных и инновационных проектах	
Владеть	Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации. Навыками организации и реализации междисциплинарных и инновационных проектов	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности		
Знать	роль правовой информации в развитии современного общества и профессиональной деятельности; виды источников права систему законодательства Российской Федерации	Правоведение
Уметь	находить и анализировать правовую информацию; использовать правовую информацию при решении конкретных жизненных ситуаций	
Владеть	практическими навыками работы со справочно-поисковыми системами Консультант Плюс и Гарант	
Знать	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. Системы регулирования возникающих общественных отношений в информационной сферы. Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.	Основы информационной безопасности
Уметь	Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. Использовать инфраструктуру единого информационного пространства РФ в личных целях. Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.	
Владеть	Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. Способами использования информационной инфраструктуры в интересах общественного развития. Методами разработки проектов нормативных документов, регламентирующих работу по защите информации	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Знать	виды тайн, закрепленные в российском законодательстве -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях -основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Организационное и правовое обеспечение информационной безопасности
Уметь	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
Владеть	навыками работы с нормативными правовыми актами -навыками подготовки деловой корреспонденции	
Знать	- основные нормативные правовые акты в области защиты информации; - основные законы о цифровых правах граждан РФ;	Основы безопасности цифрового общества
Уметь	- находить нужные источники цифровой информации и цифровые данные; - воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными	
Владеть	- способами эффективного использования полученной цифровой информации для решения профессиональных задач; - управлять цифровой информацией и данными;	
Знать	– Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. – Системы регулирования возникающих общественных отношений в информационной сферы. – Составляющие информационной сферы, представляющей собой совокупность	Производственная-практика по получению профессиональных умений и опыта

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. – Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.	профессиональной деятельности
Уметь	– Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. – Использовать инфраструктуру единого информационного пространства РФ в личных целях. – Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.	
Владеть	– Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. – Способами использования информационной инфраструктуры в интересах общественного развития. – Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.	
Знать	– Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации. – Системы регулирования возникающих общественных отношений в информационной сферы. – Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации. – Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.	Производственная-преддипломная практика
Уметь	– Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информации автоматизированных систем. – Использовать инфраструктуру единого информационного пространства РФ в личных целях. – Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.	
Владеть	– Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. – Способами использования информационной инфраструктуры в интересах общественного развития. – Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.	
ОПК-7 - способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций		
Знать:	- основные понятия о приемах первой помощи; - основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности; - характеристики опасностей природного, техногенного и социального происхождения; - государственную политику в области подготовки и защиты населения в условиях чрезвычайных ситуаций	Безопасность жизнедеятельности
Уметь:	- выделять основные опасности среды обитания человека; - оцениватьрискихреализации	
Владеть:	- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций	
Знать:	- основные понятия о приемах первой помощи; - основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности; - характеристики опасностей природного, техногенного и социального происхождения; - государственную политику в области подготовки и защиты населения в условиях	Физическая культура и спорт

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	чрезвычайных ситуаций	
Уметь:	- выделять основные опасности среды обитания человека; - оценивать риск их реализации	
Владеть:	- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций	
ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий.		
Знать	– основные определения и понятия, используемые в теории операционных систем; – современные подходы к организации и проведению научных исследований с использованием сетевых технологий; – принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;	Безопасность операционных систем
Уметь	- разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;	
Владеть	- навыками использования операционных систем, информационных систем и сетевых технологий в системах защиты информации и в учебной деятельности; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.	
Знать	Нормативные и правовые акты в области защиты информации передаваемой в сетях ЭВМ; ─ Современные технологии обеспечения информационной безопасности в сетях ЭВМ; ─ Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ	Безопасность сетей ЭВМ
Уметь	Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей; - Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети; - Разрабатывать и реализовать политику сетевой безопасности при настройке и конфигурировании сетевого оборудования.	
Владеть	Навыками работы с современными программными сканерами сетевых протоколов и сетевых уязвимостей; - Навыками решения задач по поиску неисправностей вычислительных сетей с целью выявления уязвимостей вычислительных сетей и нейтрализации обнаруженных уязвимостей; - Навыками повышения уровня защищенности вычислительных сетей и оптимизации их работы.	
Знать	принципы построения и функционирования, примеры реализаций современных операционных систем; ─ принципы работы элементов и функциональных узлов электронной аппаратуры; ─ типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	Организация ЭВМ и вычислительных систем
Уметь	применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); ─ работать с современной элементной базой электронной аппаратуры	
Владеть	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	
Знать	Принципы построения вычислительных сетей; - Классификацию сетей ЭВМ; - Принципы передачи информации по телекоммуникационным каналам связи; - Классификацию сетевого оборудования; - Принципы функционирования и основные структурные и функциональные элементы различных классов сетевого оборудования; - Семиуровневую эталонную модель взаимодействия открытых систем (модель OSI) с твердым пониманием назначения каждого из уровней модели;	Сети и системы передачи информации

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- Принципы адресации в вычислительных сетях; - Принципы организации межсетевого взаимодействия и межсетевой передачи информации.	
Уметь	Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками.	
Владеть	Профессиональным языком и терминологией предметной области (сети ЭВМ); - Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ).	
Знать	Классификацию современных программных и программно- аппаратных СЗИ. Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.	Программно-аппаратные средства обеспечения информационной безопасности
Уметь	Осуществлять сбор, обработку, анализ и систематизацию научно- технической информации в области программных и программно- аппаратных средств ЗИ и систем с применением современных информационных технологий. Основные принципы работы всех подсистем системы ИБ АС.	
Владеть	Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. Навыками администрирования системы ИБ АС.	
Знать:	Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ • Общую характеристику и структуру стандартов (ГОСТов), регламентирующих порядок проектирования АС в защищенном исполнении. • Определять потребности в технических средствах защиты и контроля	Разработка и эксплуатация защищенных автоматизированных систем
Уметь:	Осуществлять сбор, обработку, анализ и систематизацию научно- технической информации в области программных и программно- аппаратных средств ЗИ • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	• Разрабатывать требования по защите автоматизированных систем • Отображать предметную область на конкретную модель данных	
Владеть:	методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • Практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать	─ принципы построения и функционирования, примеры реализаций распределенных систем; ─ принципы работы элементов и функциональных узлов электронной аппаратуры; ─ концепции построения распределенных информационных систем	Методы проектирования систем защиты распределенных информационных систем
Уметь:	─ уметь определять особенности современных программных, технических средств и информационных технологий; ─ эксплуатировать современные программные, технические средства и информационные технологии; ─ проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	
Владеть	─ методикой эксплуатации современные программных, технических средств и информационных технологий; ─ навыками обеспечения безопасности информации с помощью типовых программных средств;	
Знать	основные информационные технологии, используемые в автоматизированных системах; - основные программные и технические средства для безопасной работы с базой данных (БД); - новые образцы программных, технических средств для БД; - системы управления базами данных; - способы и алгоритм внедрения и продуктивного использования новых программных, технических средств для БД;	Информационные технологии. Базы данных
Уметь:	работать в некоторых интегрированных средах систем управления базой данных (СУБД); - построить схему БД в программных средствах создания БД; - быстро приспособиться к работе в новых интегрированных средах СУБД;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	навыками работы на языке манипулирования БД; - методами оценки правильности проектирования БД;	
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;	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
Уметь:	– применять типовые программные средства сервисного назначения; – 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; – навыками обеспечения безопасности информации с помощью типовых программных средств; – 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	
Знать	– Классификацию современных программных и программно-аппаратных СЗИ. – Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. – Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь:	– Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	применением современных информационных технологий. – Основные принципы работы всех подсистем системы ИБ АС.	
Владеть	– Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. – Навыками администрирования системы ИБ АС.	
ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ		
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		
Знать	основные приемы и методы, связанные с поиском, изучением, обобщением и систематизациейнаучно-техническойинформации	Иностранный язык
Уметь	использовать основные приемы и методы для поиска, изучения, обобщения и систематизациинаучно-техническойинформации	
Владеть	основными приемами и методами для поиска, изучения, обобщения исистематизации научно-технической информации	
Знать	Основы построения систем обработки и передачи информации, их современное состояние развития. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. Особенности обработки информации с использованием компьютерных систем	Введение в специальность
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.	
Владеть	Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам. Основными методами научного познания в области защиты информации автоматизированных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	систем, а так же их применения к решению прикладных задач.	
Знать	– особенности обработки информации в сфере Big Data	Основы Data инжиниринга
Уметь	– обобщать, систематизировать, обеспечивать надежную инфраструктуру полученной научно-технической информации в сфере data инжиниринг.	
Владеть	– методами сбора и обобщения научно-технической информации по теоретическим сведениям, проблемам и задачам, решаемым в курсе "Data Инжиниринг", в т.ч. с использованием литературы на иностранном языке.	
Знать	основные приемы и методы, связанные с поиском, изучением, обобщением исистематизацией научно-технической информации	Иностранный язык в профессиональной деятельности
Уметь	использовать основные приемы и методы для поиска, изучения, обобщения исистематизации научно-технической информации	
Владеть	основными приемами и методами для поиска, изучения, обобщения исистематизации научно-технической информации	
Знать	– основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; – язык программирования высокого уровня (объектно-ориентированное программирование);	Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности
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	
Знать	Основы построения систем обработки и передачи информации, их современное состояние развития. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. Особенности обработки информации с использованием компьютерных систем	Научно-исследовательская работа

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно- технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.	
Владеть	Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам. Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.	
Знать	– Основы построения систем обработки и передачи информации, их современное состояние развития. – Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. – Особенности обработки информации с использованием компьютерных систем	Производственная-преддипломная практика
Уметь	– Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. – Принимать участие в исследованиях и анализе современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. – Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.	
Владеть	– Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. – Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам. – Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
ПК-2 - способностью создавать и исследовать модели автоматизированных систем.		
Знать	─ Основные информационные технологии, используемые в автоматизированных системах; ─ Классификацию современных автоматизированных систем; ─ Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем.	Основы теории оптимизации
Уметь	─ Демонстрировать способность и готовность к решению задач оптимизации применительно к различным предметным областям; ─ Определять возможность применения основных положений и методов теории оптимизации для организации мер по защите информации в автоматизированных системах; ─ Находитьоптимальныестратегии	
Владеть	Навыками использования стандартных методов теории оптимизации; ─ Навыками использования стандартных методов и моделей математического анализа, теории оптимизации; ─ Навыками использования стандартных методов и моделей математического анализа, теории оптимизации, а так же их применения к решению прикладных задач.	
Знать	Принципы и методы проектирования программно-аппаратного обеспечения; ─ Принципы и методы проектирования программно-аппаратного обеспечения; ─ Методы планирования и организации работ по защите информации	Математическое моделирование распределенных систем
Уметь	Разрабатывать и использовать профили защиты и задания по безопасности; ─ Готовить проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; ─ Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы.	
Владеть	Навыками разработки технических заданий, рабочих проектов, планов и графиков проведения работ по защите информации; ─ Навыками выполнения требований нормативно-технической документации по соблюдению установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации; ─ Навыками проектирования программных и аппаратные средств защиты информации в соответствии с техническим заданием	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	Научно-исследовательская работа
Уметь	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -применять специализированные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации − анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	
Владеть	-основами построения моделей систем передачи информации -навыками пользования библиотеками прикладных программ для решения прикладных задач -навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей -навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
Знать	-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -основные принципы моделирования и виды моделей, требования, предъявляемые к моделям -методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах -способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	Производственная-преддипломнаяпрактика
Уметь	-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные методы моделирования, исследования и верификации моделей -применять специализированные методы моделирования, исследования и верификации моделей -разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации − анализировать и оценивать угрозы информационной безопасности объекта; − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	
Владеть	-основами построения моделей систем передачи информации -навыками пользования библиотеками прикладных программ для решения прикладных задач -навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач -навыками формализации задач и постановки задач моделирования -навыками выбора и обоснования критериев эффективности функционирования моделей	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	-навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности; -навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите -методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
ПК-3 - Способностью проводить анализ защищенности автоматизированных систем.		
Знать	Основы методологии научных исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем Классификацию современных компьютерных систем. Современные способы использования компьютерных технологий для проведения исследований. Технические средства контроля эффективности мер защиты информации. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.	Основы информационной безопасности
Уметь	Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. Анализировать основные узлы и устройства современных автоматизированных систем. Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. Эффективно использовать современные компьютерные технологии для изучения предмета исследования.	
Владеть	Представлением о возможности использования информационных технологий для решения профессиональных задач. Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. Представлением о способах и методах анализа защищенности информационной	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	инфраструктуры автоматизированной системы.	
Знать	Критерии оценки эффективности и надежности средств защиты распределенных информационных систем. Принципы построения и функционирования распределенных информационных систем в защищённом исполнении. Методики анализа и контроля защищенности РИС в защищённом исполнении.	Информационная безопасность распределенных информационных систем
Уметь	Анализировать техническую и сопроводительную документацию по обеспечению ИБ. Анализировать программные и архитектурно-технические решения компонентов автоматизированных систем в защищённом исполнении. Проводить выбор технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.	
Владеть	Навыками анализа основных узлов автоматизированных систем. Навыками анализа основных узлов автоматизированных систем в защищённом исполнении. Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении	
Знать	- перечень инструментов для проведения анализа уязвимостей программного обеспечения; - базовый функционал инструментов для проведения анализа уязвимостей программного обеспечения;	Анализ уязвимостей программного обеспечения
Уметь	- применять технические средства для проведения анализа уязвимостей программного обеспечения;	
Владеть	- навыками работы с специализированным программным обеспечением для проведения анализа уязвимостей программного обеспечения	
Знать	– Основы методологии научных исследований. – Технические средства контроля эффективности мер защиты информации. – Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем – Классификацию современных компьютерных систем. – Современные способы использования компьютерных технологий для проведения исследований. – Технические средства контроля эффективности мер защиты информации.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.	
Уметь	– Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. – Анализировать основные узлы и устройства современных автоматизированных систем. – Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. – Эффективно использовать современные компьютерные технологии для изучения предмета исследования.	
Владеть	– Представлением о возможности использования информационных технологий для решения профессиональных задач. – Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. – Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. – Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.	
Знать	– Основы методологии научных исследований. – Технические средства контроля эффективности мер защиты информации. – Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем – Классификацию современных компьютерных систем. – Современные способы использования компьютерных технологий для проведения исследований. – Технические средства контроля эффективности мер защиты информации. – Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.	Производственная-преддипломная практика
Уметь	– Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Анализировать основные узлы и устройства современных автоматизированных систем. – Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах. – Эффективно использовать современные компьютерные технологии для изучения предмета исследования.	
Владеть	– Представлением о возможности использования информационных технологий для решения профессиональных задач. – Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности. – Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности. – Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.	
ПК-4 –способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		
Знать	-Правила, процедуры, практические приемы, руководящие принципы, методы, средства для построения модели угроз и модели нарушителя информационной безопасности автоматизированной системы -Методы и средства разработки моделей на основе теории графов	Теория графов и ее приложения
Уметь	-Использовать технологии автоматизированного проектирования информационных систем -Применять методы теории графов для построения модели нарушителя в автоматизированных системах	
Владеть	-Навыками применения графовых алгоритмов для определения ресурсов, необходимых для обеспечения безопасности информационной системы -Методами построения моделей для контроля эффективности мер защиты информации	
Знать	основные источники угроз ИБ; классификацию угроз информационной безопасности; Типовую модель угроз информационной безопасности Нормативно-методические документы в области моделирования угроз,	Моделирование угроз информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах;	
Уметь	Разрабатывать частную модель угроз автоматизированной системы Определять актуальные угрозы для автоматизированной системы; разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.	
Владеть	Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; Навыками разработки частных моделей угроз	
Знать	- нормативные и правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; - основы функционирования ГосСОПКА; - понятия объектов и субъектов КИИ;	Обеспечение информационной безопасности критической информационной инфраструктурой
Уметь	- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ; - способы реализации угроз безопасности и возможные последствия от их реализации; - определять требования по устранению возможных уязвимостей, приводящих к возникновению угроз безопасности информации;	
Владеть	- навыками работы с нормативными и правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ; - навыками работы с информационными базами данных, содержащими информацию по угрозам безопасности информации и уязвимостями ПО значимых объектов КИИ; - навыками выявления и анализа угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;	
Знать	– Основные источники угроз ИБ и факторы, необходимые для учета при разработке модели ИБ – классификацию угроз информационной безопасности	Производственная-практика по получению

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– перечень нормативных документов – Способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	профессиональных умений и опыта профессиональной деятельности
Уметь	– анализировать и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных систем	
Владеть	– Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; – навыками семантического моделирования данных – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
Знать	– Основные источники угроз ИБ и факторы, необходимые для учета при разработке модели ИБ – классификацию угроз информационной безопасности – перечень нормативных документов – Способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах	Производственная-преддипломная практика
Уметь	– анализировать и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных систем	
Владеть	– Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; – навыками семантического моделирования данных – методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
ПК-5 – способностью проводить анализ рисков информационной безопасности автоматизированной системы		
Знать	методологию анализа рисков информационной безопасности; - методики определения	Анализ рисков

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информационно-технологических ресурсов, подлежащих защите; - способы применения анализа рисков информационной безопасности при работе над междисциплинарными проектами; - перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами.	информационной безопасности
Уметь	применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами; - выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.	
Владеть	- терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите; - навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.	
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих защите – способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами – выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	
Знать	– методологию анализа рисков информационной безопасности – методики определения информационно-технологических ресурсов, подлежащих защите – способы применения анализа рисков в информационной безопасности при работе над междисциплинарными проектами – перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами	Производственная-преддипломная практика
Уметь	– применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами – выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	
Владеть	– терминологией, используемой при анализе особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите – навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности		
Знать	Основные информационные технологии, используемые в автоматизированных системах. Сущность и понятие информационной безопасности и характеристику ее составляющих. Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.	Основы информационной безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. Принимать участие в исследованиях и анализе современной научно- технической информации по информационной безопасности. Анализировать современную научно-техническую информацию по информационной безопасности. Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	
Владеть	Основными методами научного познания в области защиты информации. Навыками участия в проведении исследовательских работ по информационной безопасности. Профессиональной терминологией в области информационной безопасности. Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах	
Знать	─ источники и классификацию угроз информационной безопасности; ─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; ─ основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	Методы проектирования систем защиты распределенных информационных систем
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 и документирования распределенных информационных систем; ─ методами формирования требований по защите информации; ─ навыками анализа основных узлов и устройств современных автоматизированных систем; ─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать	методологию и этапы проектирования базы данных; - метод «сущность-связь» для проектирования БД; -методы и подходы создания инфологической модели БД;	Информационные технологии. Базы данных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; - применять средства обеспечения безопасности баз данных	
Владеть	основами проектирования БД; - навыками отображения предметной области на конкретную модель данных;	
Знать	источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	Научно-исследовательская работа
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; навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать	- область применения IoT-систем; - архитектуру IoT-систем; - принципы построения систем на базе IoT-устройств;	Безопасность Интернета вещей
Уметь	- планировать работы по проектированию сложных IoT-систем; - проектировать структуру и архитектуру системы на базе IoT- устройств с использованием современных технологий	
Владеть	- навыками проектирования, тестирования и отладки систем на базе IoT-устройств;	
Знать	Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения.	Анализ уязвимостей программного

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	- проводить анализ уязвимостей программного обеспечения; - выполнять реверс инжиниринг программного обеспечения;	обеспечения
Владеть	- навыками противодействия атакам на программное обеспечение;	
Знать	– Основные информационные технологии, используемые в автоматизированных системах. – Сущность и понятие информационной безопасности и характеристику ее составляющих. – Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам. – Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. – Анализировать современную научно-техническую информацию по информационной безопасности. – Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	
Владеть	– Основными методами научного познания в области защиты информации. – Навыками участия в проведении исследовательских работ по информационной безопасности. – Профессиональной терминологией в области информационной безопасности. – Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах	
Знать	– Основные информационные технологии, используемые в автоматизированных системах. – Сущность и понятие информационной безопасности и характеристику ее составляющих. – Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.	Производственная-преддипломная практика
Уметь	– Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности. – Анализировать современную научно-техническую информацию по информационной безопасности. – Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе	
Владеть	– Основными методами научного познания в области защиты информации. – Навыками участия в проведении исследовательских работ по информационной безопасности. – Профессиональной терминологией в области информационной безопасности. – Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах	
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ		
Знать	-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	Организационное и правовое обеспечение информационной безопасности
Уметь	-разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
Владеть	-способностью разрабатывать научно-техническую документацию	
Знать	нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	Научно-исследовательская работа
Уметь	разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
Владеть	способностью разрабатывать научно-техническую документацию	
Знать	– нормативные правовые акты и нормативные методические документы в области	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	обеспечения информационной безопасности, структуру научно-технических отчетов	практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
Владеть	– способностью разрабатывать научно-техническую документацию	
Знать	– нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	Производственная-преддипломная практика
Уметь	– разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
Владеть	– способностью разрабатывать научно-техническую документацию	
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем		
Знать	─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ современную нормативно-правовую базу создания защищенных распределенных информационных систем; ─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	Методы проектирования систем защиты распределенных информационных систем
Уметь	─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; ─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем	
Владеть	─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; ─ навыками разработки комплексной инфраструктуры защищенной информационной системы; ─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации	
Знать	─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– современную нормативно-правовую базу создания защищенных распределенных информационных систем; – инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	практика по получению профессиональных умений и опыта профессиональнойдеятельности
Уметь	– разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; – применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем	
Владеть	– методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – навыками разработки комплексной инфраструктуры защищенной информационной системы; – навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации	
Знать	– методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – современную нормативно-правовую базу создания защищенных распределенных информационных систем; – инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей	Производственная-преддипломная практика
Уметь	– разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; – применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем	
Владеть	– методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем; – навыками разработки комплексной инфраструктуры защищенной информационной системы; – навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации	
ПК-9. Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	Основные элементы персонального компьютера и их функциональное назначение, базовые топологии автоматизированных систем;	Организация ЭВМ и

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	─ Логическую, функциональную и структурную схему персонального компьютера, устройства организующие работу вычислительных систем; ─ Логику работы центрального процессора при выполнении вычислений и при передаче данных между ЦП и периферийными устройствами ПК	вычислительных систем
Уметь	Определять требуемый перечень компонентов ПК под конкретное техническое задание; ─ Определять основные неисправности ПК и подключенных к нем устройств; ─ Проектировать одноранговые вычислительные сети	
Владеть	Навыками сборки ПК из отдельных комплектующих; ─ Навыками работы с осциллографом; ─ Навыками настройки адаптеров сетевых подключений	
Знать	Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем • Основные принципы построения защищенных распределенных компьютерных систем • Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. • Современные принципы построения архитектуры ИС.	Разработка и эксплуатация защищенных автоматизированных систем
Уметь	Осуществлять анализ несложных процессов проектирования создавать дополнительные средства защиты; • Осуществлять анализ и оптимизацию несложных процессов проектирования • Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы • разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	
Владеть	Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации • Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации • Определять уровни защищенности и доверия программно- аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	автоматизированных систем • Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации • Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	
Знать	варианты интерпретации бинарного потока данных; - структуру пакетов данных транспортного уровнять протокола TCP;	Технология построения защищенных распределенных приложений
Уметь	выполнять анализ данных транспортного уровнять протокола TCP при помощи специализированного программного обеспечения	
Владеть	-навыками сериализации данных	
Знать	- Стандарты в области оценки защищенности компьютерных систем - Критерии оценки безопасности информационных технологий - Методы оценки защищенности компьютерных систем	Методы и стандарты оценки защищенности компьютерных систем
Уметь	- Проводить анализ защищенности компьютерных систем - Выполнять оценку систем информационной безопасности - Составлять диаграммы информационной безопасности	
Владеть	- Методами оценки защищенности компьютерных систем - Методами тестирования защищенности компьютерных систем	
Знать	– Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем – Основные принципы построения защищенных распределенных компьютерных систем – Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. – Современные принципы построения архитектуры ИС.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Осуществлять анализ несложных процессов проектирования создавать дополнительные средства защиты; – Осуществлять анализ и оптимизацию несложных процессов проектирования – Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	
Владеть	– Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации – Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации – Определять уровни защищенности и доверия программно-аппаратных средств защиты информации – Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем – Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации – Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	
Знать	– Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем – Основные принципы построения защищенных распределенных компьютерных систем – Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. – Современные принципы построения архитектуры ИС.	Производственная-преддипломная практика
Уметь	– Осуществлять анализ несложных процессов проектирования создавать дополнительные средства защиты; – Осуществлять анализ и оптимизацию несложных процессов проектирования – Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы – разрабатывать технические задания на создание подсистем информационной	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	
Владеть	– Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации – Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации – Определять уровни защищенности и доверия программно-аппаратных средств защиты информации – Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем – Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации – Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах	
ПК-10 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности.		
Знать	Способы разработки сложного программного обеспечения. Эффективные способы реализации структур данных и конкретных алгоритмов при решении различных задач. Требования, предъявляемые к разработке внешних спецификаций, для разрабатываемого программного обеспечения.	Языки программирования
Уметь	Планировать разработку сложного программного обеспечения. Проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении различных задач. Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения.	
Владеть	Навыками разработки типового программного обеспечения.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Навыками разработки внешней спецификации для разрабатываемого программного обеспечения. Навыками разработки сложного программного обеспечения.	
Знать	Современные технологии программирования. Области и особенности применения языков программирования высокого уровня; Основные виды интегрированных сред разработки программного обеспечения. Основные методы эффективного кодирования. Способы обработки исключительных ситуаций; Современные технологии и методы программирования, предназначенные для создания прикладных программ.	Технологии и методы программирования
Уметь	Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; Работать с основными средами интегрированной разработки программного обеспечения; Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; Реализовывать разработанную структуру классов для задач предметной области.	
Владеть	Навыками реализации алгоритмов на языках программирования высокого уровня; Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. Технологиями программирования распределенных автоматизированных систем;Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	
Знать	основы теории электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры	Электроника и схемотехника
Уметь	применять на практике методы анализа электрических цепей; работать с современной элементной базой электронной аппаратуры; использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации	
Владеть	навыками работы с программными средствами схемотехнического моделирования; навыками чтения принципиальных схем, построения временных диаграмм и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	восстановления алгоритма работы узла, устройства и системы по комплексу документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы	
Знать	Виды сетевых топологий; - Принципы передачи информации по телекоммуникационным каналам; - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - Классификациюсетевыхпротоколов.	Сети и системы передачи информации
Уметь	Самостоятельно диагностировать неисправности сетей ЭВМ; - Контролировать безотказное функционирование сетей ЭВМ; - Осуществлять подбор инструментальных и программных средств тестирования сетей ЭВМ; - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.	
Владеть	Методиками проектирования топологии вычислительных сетей; - Навыками определения и поиска неисправностей в сетях ЭВМ; - Навыкаминастройкисетевогооборудования	
Знать	Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ. Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.	Программно-аппаратные средства обеспечения информационной безопасности
Уметь	Исследовать эффективность контрольных проверок работоспособности применяемых программно-аппаратных средств защиты информации. Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей ИБ АС.	
Владеть	Навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации. Навыками использования программно-аппаратных средств обеспечения ИБ АС. Навыками анализа программных, архитектурно-технических и схемотехнических решении компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Знать	- современные методы и средства защиты информации в компьютерных системах; - принципы и способы использования существующих средств ЗИ в компьютерных системах; - принципы применения современных методов оценки безопасности компьютерных систем;	Методы и стандарты оценки защищенности компьютерных систем
Уметь	- выявлять угрозы и определять их актуальность для современных компьютерных систем; - применять современные методы оценки безопасности компьютерных систем;	
Владеть	- практическими навыками применения методов обеспечения безопасности компьютерных систем; - навыками применения современных методов оценки безопасности компьютерных систем.	
Знать	– характеристики и область применимости базовых электронных компонентов; – схемотехнику основных электронных узлов радиотехнических систем; – программное обеспечение для разработки систем передачи информации в целом и отдельных её узлов.	Основы радиотехники
Уметь	– создавать имитационные модели радиотехнических систем передачи информации с помощью специализированного программного обеспечения; – проводить анализ систем передачи информации в целом; – разрабатывать системы передачи информации в целом и отдельных её узлов; – создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.	
Владеть	– навыками проектирования и создания отдельных элементов и узлов радиотехнических устройств; – методами анализа работоспособности электронных узлов радиотехнических устройств с помощью специализированного программного обеспечения; – методами разработки системы передачи информации в целом и отдельных её узлов	
Знать	– характеристики и область применимости базовых электронных компонентов; – схемотехнику основных электронных узлов систем передачи информации; – программное обеспечение для разработки систем передачи информации в целом и отдельных её узлов.	Физические основы передачи информации
Уметь	– создавать имитационные модели систем передачи информации с помощью	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	специализированного программного обеспечения; − проводить анализ систем передачи информации в целом; − разрабатывать системы передачи информации в целом и отдельных её узлов; − создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.	
Владеть	− навыками проектирования и создания отдельных элементов и узлов устройств связи; − методами анализа работоспособности электронных узлов устройств связи с помощью специализированного программного обеспечения; − методами разработки системы передачи информации в целом и отдельных её узлов	
Знать	Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах; - Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах.	Виртуальные сети
Уметь	Создавать защищенные вычислительные сети с применением виртуализации; - Применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях.	
Владеть	Навыками разработки, документирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению безопасности	
Знать	– Современные технологии программирования. – Области и особенности применения языков программирования высокого уровня; – Основные виды интегрированных сред разработки программного обеспечения. – Основные методы эффективного кодирования. – Способы обработки исключительных ситуаций; – Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.	Защита программного обеспечения
Уметь	– Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач; – Работать с основными средами интегрированной разработки программного обеспечения;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – Реализовывать разработанную структуру классов для задач предметной области.	
Владеть	– Навыками реализации алгоритмов на языках программирования высокого уровня; – Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. – Технологиями программирования распределенных автоматизированных систем; – Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	
Знать	– Современные технологии программирования. – Области и особенности применения языков программированиявысокого уровня; – Основные виды интегрированных сред разработки программного обеспечения. – Основные методы эффективного кодирования. – Способы обработки исключительных ситуаций; – Современные технологии и методы программирования, предназначенные для создания прикладных программ.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Реализовывать на языке высокого уровня алгоритмы решенияпрофессиональных задач; Работать с основными средами интегрированной разработки программногообеспечения; – Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – Реализовывать разработанную структуру классов для задач предметной области.	
Владеть	– Навыками реализации алгоритмов на языкахпрограммирования высокого уровня; – Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. – Технологиями программирования распределенных автоматизированных систем;Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	
Знать	– Современные технологии программирования.	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Области и особенности применения языков программированиявысокого уровня; – Основные виды интегрированных сред разработки программного обеспечения. – Основные методы эффективного кодирования. – Способы обработки исключительных ситуаций; – Современные технологии и методы программирования, предназначенные для создания прикладных программ.	преддипломная практика
Уметь	– Реализовывать на языке высокого уровня алгоритмы решенияпрофессиональных задач; Работать с основными средами интегрированной разработки программногообеспечения; – Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; – Реализовывать разработанную структуру классов для задач предметной области.	
Владеть	– Навыками реализации алгоритмов на языкахпрограммирования высокого уровня; – Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. – Технологиями программирования распределенных автоматизированных систем;Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.	
ПК-11способностью разрабатывать политику информационной безопасности автоматизированной системы		
Знать	задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;	Управление информационной безопасностью
Уметь	разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.	
Владеть	навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
Знать	- задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
Знать	- задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;	Производственная-преддипломная практика
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
ПК-12способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы		
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз.	Управление информационной безопасностью
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.	
Владеть	навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.	
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС;	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- методы анализа процессов для определения актуальных угроз.	
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.	
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
ПК-13. способностью участвовать в проектировании средств защиты информации автоматизированной системы		
Знать	- способы организации обмена данными при помощи технологии RPC; - способы организации обмена данными при помощи технологии RMC; - способы организации обмена данными при помощи очередей; - функционал платформы .Net в части организации обмена данными; - функционал Run-TimeEngine; - криптографические протоколы обмена информацией;	Технология построения защищенных распределенных приложений
Уметь	разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи на языке C#; - разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи в среде разработки LabVIEW;	
Владеть	навыками оформления программной документации по ЕСПД;	
Знать	- способы организации обмена данными при помощи технологии RPC; - способы организации обмена данными при помощи технологии RMC; - способы организации обмена данными при помощи очередей; - функционал платформы .Net в части организации обмена данными; - функционал Run-Time Engine; - криптографические протоколы обмена информацией;	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;	
Владеть	- навыками оформления программной документации по ЕСПД;	
Знать	- способы организации обмена данными при помощи технологии RPC;	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- способы организации обмена данными при помощи технологии RMC; - способы организации обмена данными при помощи очередей; - функционал платформы .Net в части организации обмена данными; - функционал Run-Time Engine; - криптографические протоколы обмена информацией;	преддипломная практика
Уметь	- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;	
Владеть	- навыками оформления программной документации по ЕСПД;	
ПК-14 - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.		
Знать	• принципы обработки временных рядов и изображений.	Физика
Уметь	обрабатывать экспериментальные данные (построение гистограмм, построение линий регрессии, построения автокорреляционных и спектральных функций, взаимно корреляционных функций, определение выбросов, сбоев)	
Владеть	практическими навыками оформления результатов научной и исследовательской деятельности с учётом точности и дисперсии опытных данных, исключением выбросов, сбоев	
Знать:	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. • методы шифрования, использующие классические симметричные алгоритмы, • методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, • методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. • общие принципы действия шифровальной машины Энигма • общие принципы шифрования, используемые в алгоритме симметричного шифрования AES • принципы шифрования информации с помощью биграммного шифра Плейфера • Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.	Криптографические методы защиты информации
Уметь:	исследовать различные методы защиты текстовой информации и их стойкости на основе	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	подбора ключей • Участвовать в настройке криптографических средств обеспечения информационной безопасности. • Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. • Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.	
Владеть:	Техникой настройки криптографических средств обеспечения информационной безопасности. • Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. • Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	
Знать	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации. Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.	Техническая защита информации
Уметь	Участвовать в настройке технических средств обеспечения информационной безопасности. Самостоятельно настраивать технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. Применять технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.	
Владеть	Техникой настройки технических средств обеспечения информационной безопасности.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	
Знать:	Виды программных и программно-аппаратных средств защиты информации. Принципы администрирования системы ИБ АС. Способы контрольных проверок работоспособности и эффективности применяемых программных и программно- аппаратных СЗИ.	Программно-аппаратные средства обеспечения информационной безопасности
Уметь:	Самостоятельно настраивать программные и программно- аппаратные средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно- аппаратных СЗИ. Применять программные и программно-аппаратные средства обеспечения ИБ.	
Владеть:	Техникой настройки программных и программно-аппаратных средств обеспечения ИБ. Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС. Навыками анализа архитектурно-технических и схемотехнических решений компонентов АС с целью выявления потенциальных уязвимостей ИБ АС	
Знать	– Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. – методы шифрования, использующие классические симметричные алгоритмы, – методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, – методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. – общие принципы действия шифровальной машины Энигма – общие принципы шифрования, используемые в алгоритме симметричного шифрования	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	AES – принципы шифрования информации с помощью биграммного шифра Плейфера – Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.	
Уметь	– исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей – Участвовать в настройке криптографических средств обеспечения информационной безопасности. – Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. – Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.	
Владеть	– Техникой настройки криптографических средств обеспечения информационной безопасности. – Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. – Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	
Знать:	– Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. – методы шифрования, использующие классические симметричные алгоритмы, – методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, – методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера.	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– общие принципы действия шифровальной машины Энигма – общие принципы шифрования, используемые в алгоритме симметричного шифрования AES – принципы шифрования информации с помощью биграммного шифра Плейфера – Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.	
Уметь:	– исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей – Участвовать в настройке криптографических средств обеспечения информационной безопасности. – Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. – Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.	
Владеть:	– Техникой настройки криптографических средств обеспечения информационной безопасности. – Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. – Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	
ПК-15. Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем		
Знать	Модель жизненного цикла и порядок создания АС; • структуру, порядок составления, оформления и утверждения Технического задания по созданию АС • Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и	Разработка и эксплуатация защищенных автоматизированных

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия	систем
Уметь	Анализировать и оценивать угрозы информационной безопасности объекта • Определять потребности в технических средствах защиты и контроля • Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов • Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных • Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем • Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	
Владеть	методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем • практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать	способы организации автоматизированных систем; - подходы к проведению сертификации средств защиты информационной безопасности;	Методы мониторинга информационной безопасности АС
Уметь	составлять регламент испытаний средств защиты информации автоматизированных систем;	
Владеть	навыками применения, специализированного ПОдля проведения мероприятий при сертификации средств защиты информации автоматизированных систем;	
Знать	– Модель жизненного цикла и порядок создания АС; – структуру, порядок составления, оформления и утверждения Технического задания по созданию АС – Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	доверия	
Уметь	– Анализировать и оценивать угрозы информационной безопасности объекта – Определять потребности в технических средствах защиты и контроля – Планировать индивидуально-групповою структуру пользователей информационных систем и структуру разделяемых (коллективных) информационных ресурсов – Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных – Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем – Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	
Владеть	– методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем – практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать	– Модель жизненного цикла и порядок создания АС; – структуру, порядок составления, оформления и утверждения Технического задания по созданию АС – Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия	Производственная-преддипломная практика
Уметь	– Анализировать и оценивать угрозы информационной безопасности объекта – Определять потребности в технических средствах защиты и контроля – Планировать индивидуально-групповою структуру пользователей информационных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	систем и структуру разделяемых (коллективных) информационных ресурсов – Разрабатывать требования по защите компьютерных систем отображать предметную область на конкретную модель данных – Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем – Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	
Владеть	– методиками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем – практическими навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем	
Знать:	– правила оформления научно-технической документации; – принципы работы и параметры используемого оборудования для проведения экспериментально-исследовательских работ; – типовые схемы экспериментального исследования основных электронных приборов и устройств	Тестирование систем защиты информации автоматизированных систем
Уметь:	– составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия; – проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия – проводить анализ сертификата соответствия.	
Владеть:	– терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспериментально-исследовательских работ; – нормативно-правовой базой в области сертификации средств защиты информации	
ПК-16 - способность участвовать в проведении экспериментально-исследовательских работ при аттестации		

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
автоматизированных систем с учетом нормативных документов по защите информации		
Знать	Средства анализа информационной безопасности; ─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации.	Методы выявления нарушений информационной безопасности
Уметь	Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.	
Владеть	Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.	
Знать	─ Средства анализа информационной безопасности; ─ Классификацию систем защиты информации; ─ Средства организации аттестации по требованиям безопасности информации.	Аттестация АИС
Уметь	─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов; ─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.	
Владеть	─ Навыками использования средств анализа информационной безопасности; ─ Навыками проведения аттестации в соответствии с существующими нормативами.	
Знать	Средства анализа информационной безопасности; Классификацию систем защиты информации; Средства организации аттестации ВП по требованиям безопасности информации.	Научно-исследовательская работа
Уметь	Принимать участие в исследованиях аттестации системы защиты информации; Принимать участие в исследованиях и анализе аттестации системы защиты информации; Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.	
Владеть	Навыками использования средств анализа информационной безопасности; Навыками участия в проведении экспериментально- исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты информации; – Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.	
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.	Производственная-преддипломная практика
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты информации; – Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.	
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	
Знать	– Средства анализа информационной безопасности; – Классификацию систем защиты информации; – Средства организации аттестации ВП по требованиям безопасности информации.	Тестирование систем защиты информации автоматизированных систем
Уметь	– Принимать участие в исследованиях аттестации системы защиты информации; – Принимать участие в исследованиях и анализе аттестации системы защиты информации; – Проводить научно-исследовательские работы при аттестации системы защиты информации с	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	учетом требований к обеспечению информационной безопасности.	
Владеть	– Навыками использования средств анализа информационной безопасности; – Навыками проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; – Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.	
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.		
Знать	Классификацию технических средств перехвата информации Возможности технических средств перехвата информации Организацию защиты информации от утечки по техническим каналам на объектах информатизации	Техническая защита информации
Уметь	Классифицировать технические средства перехвата информации. Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации Выявлять каналы утечки информации Проводить контроль эффективности мер по защите информации техническими средствами	
Владеть	Средствами технической защиты информации. Методами технической защиты информации. Навыками проведения проверки защищенности информации и эффективности мер по защите информации	
Знать	перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;	Методы мониторинга информационной безопасности АС
Уметь	применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов	
Владеть	навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе	
Знать	– Классификацию технических средств перехвата информации – Возможности технических средств перехвата информации	Производственная-практика по

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Организацию защиты информации от утечки по техническим каналам на объектах информатизации.	получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Классифицировать технические средства перехвата информации. – Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации – Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.	
Владеть	– Средствами технической защиты информации. – Методами технической защиты информации. – Методами и средствами технической защиты информации.	
Знать	– Классификацию технических средств перехвата информации – Возможности технических средств перехвата информации – Организацию защиты информации от утечки по техническим каналам на объектах информатизации.	Производственная-преддипломная практика
Уметь	– Классифицировать технические средства перехвата информации. – Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации – Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.	
Владеть	– Средствами технической защиты информации. – Методами технической защиты информации. – Методами и средствами технической защиты информации.	
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности		
Знать	– основы принятия управленческих решений	Основы управленческой деятельности
Уметь	– организовывать работу малых коллективов исполнителей	
Владеть	– навыками управления поведением человека в организации	
Знать	Основные меры по защите информации в автоматизированных системах. Принципы организации и структура систем защиты информации программного обеспечения	Основы

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	автоматизированных систем. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Принципы организации работы малых коллективов исполнителей.	информационной безопасности
Уметь	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	
Владеть	Профессиональной терминологией в области информационной безопасности. Навыками участия в проведении исследовательских работ по информационной безопасности. Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.	
Знать	организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации -организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	Организационное и правовое обеспечение информационной безопасности
Уметь	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров	
Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов	
Знать	– Основные меры по защите информации в автоматизированных системах. – Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. – Принципы организации работы малых коллективов исполнителей.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. – Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. – Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	
Владеть	– Профессиональной терминологией в области информационной безопасности. – Навыками участия в проведении исследовательских работ по информационной безопасности. – Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.	
Знать	– Основные меры по защите информации в автоматизированных системах. – Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. – Принципы организации работы малых коллективов исполнителей.	Производственная-преддипломная практика
Уметь	– Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. – Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	
Владеть	– Профессиональной терминологией в области информационной безопасности. – Навыками участия в проведении исследовательских работ по информационной безопасности. – Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.	
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		
Знать	нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации	Управление информационной безопасностью
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС	
Владеть	навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
Знать	- нормативные методические документы ФСТЭК России в области ИБ АС; - основные угрозы безопасности информации и модели нарушителя в АС; - способы оптимизации систем управления информационной безопасности (СУИБ).	Системы управления информационной безопасностью
Уметь	- анализировать применяемые инструменты в области проектирования и управления ИБ с учетом стоимости и категорирования защищаемых объектов; - обосновывать целесообразность применяемых мер по обеспечению ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	
Владеть	- навыками расследования инцидентов ИБ;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- навыками сбора и анализа исходных данных, проведение обследования бизнес-процессов компании, входящих в область действия СУИБ; - навыками оценки активов (первичных и вторичных) компании, входящих в область действия СУИБ; - навыками определения владельцев и ценности активов;	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.	Производственная-преддипломная практика
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности.		
Знать	Основы организационного и правового обеспечения ИБ. Основные нормативные и правовые акты в области обеспечения ИБ. Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ.	Информационная безопасность

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Методики проектирования АС в защищенном исполнении.	распределенных информационных систем
Уметь	Реализовывать разработанную автоматизированную систему с учетом требований ИБ. Организовывать реализацию разработанной АС с учетом требований информационной безопасности. Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.	
Владеть	Навыками разработки автоматизированных систему с учетом требований ИБ. Навыками контроля разработки АС с учетом требований ИБ. Навыками контроля эффективности применения разработанной АС в защищенном исполнении. Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении	
Знать	– Основы организационного и правового обеспечения ИБ. – Основные нормативные и правовые акты в области обеспечения ИБ. – Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. – Методики проектирования АС в защищенном исполнении.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Реализовывать разработанную автоматизированную систему с учетом требований ИБ. – Организовывать реализацию разработанной АС с учетом требований информационной безопасности. – Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. – Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.	
Владеть	– Навыками разработки автоматизированных систему с учетом требований ИБ. – Навыками контроля разработки АС с учетом требований ИБ. – Навыками контроля эффективности применения разработанной АС в защищенном исполнении. – Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении.	
Знать	– Основы организационного и правового обеспечения ИБ.	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Основные нормативные и правовые акты в области обеспечения ИБ. – Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ. – Методики проектирования АС в защищенном исполнении.	преддипломная практика
Уметь	– Реализовывать разработанную автоматизированную систему с учетом требований ИБ. – Организовывать реализацию разработанной АС с учетом требований информационной безопасности. – Готовить сопроводительную документацию к разработанной АС в защищенном исполнении. – Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.	
Владеть	– Навыками разработки автоматизированных систему с учетом требований ИБ. – Навыками контроля разработки АС с учетом требований ИБ. – Навыками контроля эффективности применения разработанной АС в защищенном исполнении. – Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении.	
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем		
Знать	основные меры по защите информации в автоматизированных системах (организационные, правовые); автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Организационное и правовое обеспечение информационной безопасности
Уметь	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия разрабатывать предложения по совершенствованию системы управления ИБ	
Владеть	методами организации и управления деятельностью служб защиты информации на предприятии	
Знать	─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; ─ организацию работы и	Методы проектирования

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	систем защиты распределенных информационных систем
Уметь	─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; ─ 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; ─ нормативными требованиями по защите информации; ─ навыками организации и обеспечения режима секретности	
Знать	– основные меры по защите информации в автоматизированных системах (организационные, правовые); – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия – разрабатывать предложения по совершенствованию системы управления ИБ	
Владеть	– методами организации и управления деятельностью служб защиты информации на предприятии	
Знать	– основные меры по защите информации в автоматизированных системах (организационные, правовые); – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	– разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия – разрабатывать предложения по совершенствованию системы управления ИБ	
Владеть	– методами организации и управления деятельностью служб защиты информации на предприятии	
Знать	– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; – нормативные правовые акты в области защиты информации; – основные методы управления проектами в области информационной безопасности.	Разработка эксплуатационной документации на системы защиты информации автоматизированных систем
Уметь	– разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем; – анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; – проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.	
Владеть	– методами анализа технической документации информационной инфраструктуры автоматизированной системы; – навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.	
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации		
Знать	основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.	Управление информационной безопасностью

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
Знать	- принципы разработки политики информационной безопасности компании/организации; - области действия СУИБ;	Системы управления информационной безопасностью
Уметь	- разрабатывать частные Политики ИБ; - определять цели и механизмы контроля обработки рисков ИБ и оценки их применимости для конкретного решения;	
Владеть	- навыками обучение и повышение осведомленности персонала предприятия/организации в области обеспечения безопасности информации; - навыками документирование процессов управления ИБ (политики, процедуры, записи)	
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- принципы формирования политики информационной безопасности организации.	
Уметь	- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.	
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	- правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей сетей ЭВМ;	Безопасность операционных систем
Уметь	- реализовывать политику безопасности операционной системы; - сформировать комплекс мер для обеспечения информационной безопасности автоматизированной системы;	
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности объектов информатизации. - навыками эксплуатации операционных систем и локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;	
Знать	- Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним; - Основные принципы методик противодействия перехвату и	Безопасность сетей ЭВМ

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ; - Классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации.	
Уметь	Применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ; ─ Определять основные угрозы безопасности в сетях ЭВМ; ─ Контролировать безотказное функционирование средств защиты информации в сетях ЭВМ; ─ Осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ; ─ Разрабатывать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой информации в сетях ЭВМ.	
Владеть	Методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; ─ Навыками настройки протоколов безопасности на современном сетевом оборудовании; ─ Приемами определения и классификации сетевых атак; ─ Методологией составления политик сетевой безопасности	
Знать	Методы формирования требований по защите информации, обрабатываемой в СУБД. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Организационные меры по защите информации, обрабатываемой в СУБД.	Безопасность систем баз данных
Уметь	Использовать методы формирования требований по защите информации, обрабатываемой в СУБД. Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД. Организовывать безопасность АРМ, на которых установлена СУБД.	
Владеть	Методами формирования требований по защите информации, обрабатываемой в СУБД. Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД.	
Знать	- правила, процедуры, практические приемы, руководящие принципы, методы,	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	средства) для обеспечения информационной безопасности автоматизированной системы - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей сетей ЭВМ;	практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- реализовывать политику безопасности операционной системы; - сформировать комплекс мер для обеспечения информационной безопасности автоматизированной системы;	
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности объектов информатизации. - навыками эксплуатации операционных систем и локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;	
Знать	- правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей сетей ЭВМ;	Производственная-преддипломная практика
Уметь	- реализовывать политику безопасности операционной системы; - сформировать комплекс мер для обеспечения информационной безопасности автоматизированной системы;	
Владеть	- навыками формальной постановки задачи обеспечения информационной безопасности объектов информатизации. - навыками эксплуатации операционных систем и локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;	
Знать	– основные меры по защите информации в автоматизированных системах; – особенности защиты информации в автоматизированных системах управления технологическими процессами; – угрозы безопасности, информационные воздействия, критерии оценки защищенности и	Разработка эксплуатационной документации на системы защиты

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	методы защиты информации в автоматизированных системах.	информации автоматизированных систем
Уметь	– определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах; – Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	
Владеть	– методами анализа защищенности информационной инфраструктуры автоматизированной системы; – навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;	
ПК-24. Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности		
Знать	- методы повышения уровня безопасности программного обеспечения;	Анализ уязвимостей программного обеспечения
Уметь	- выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять компоненты программного обеспечения, не обеспечивающие требуемый уровень информационной безопасности;	
Владеть	- навыками определения возможных векторов атаки на программное обеспечение	
Знать	- понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; - общие требования по обеспечения безопасности значимых объектов КИИ; - подходы категорирования значимости объектов КИИ;	Обеспечение информационной безопасности критической информационной инфраструктурой
Уметь	- определять категории значимых объектов КИИ и оформлять полученные результаты; - определять структуру системы безопасности значимого объекта КИИ; - определят требования по обеспечения безопасности значимых объектов КИИ; - определять требования к параметрам настройки программных и программно-аппаратных средств защиты информации (СЗИ);	
Владеть	- навыками установки и настройки СЗИ, обрабатываемой объектами КИИ; - навыками подбора средств СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;	
Знать	- Технические требования к испытательной лаборатории;	Анализ безопасности

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- Методологией тестирования безопасности информационных технологий.	информационных технологий
Уметь	- Развертывать уязвимые информационно-технологических ресурсы автоматизированной системы.	
Владеть	-Навыками анализа безопасности информационно-технологических ресурсов автоматизированной системы.	
Знать	-основные понятия предметной области построения систем организационного управления – основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы в области защиты информации -основные информационные технологии, используемые в автоматизированных системах; -передовой опыт по внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения их эффективности	Информационная безопасность систем организационного управления
Уметь	-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления - моделировать потоки информации и документооборот, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности -разрабатывать эксплуатационную документацию для систем организационного управления с учетом требований информационной безопасности	
Владеть	-навыками применения современных информационных технологий с учетом требований информационной безопасности в системах организационного управления (ОУ) -навыками подготовки инструкций по эксплуатации систем организационного управления с учетом требований информационной безопасности	
Знать	- основные понятия предметной области систем электронного документооборота -основные информационные технологии, используемые в автоматизированных системах; – принципы построения и функционирования, примеры реализаций систем электронного документооборота; нормативные правовые акты в области защиты информации	Защита электронного документооборота
Уметь	-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем электронного документооборота - моделировать потоки информации и документов, в корпоративных информационных	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	системах и осуществлять их оценивание с точки зрения информационной безопасности -готовить научно-технические отчеты, обзоры, публикации по теме предметной области	
Владеть	-навыками применения современных информационных технологий для поиска, прохождения, обработки, учета и рассылки документов внутри систем электронного документооборота -навыками моделирования потоков информации в корпоративных информационных системах и выявления актуальных угроз ИБ	
Знать	Информационно-технологические ресурсы автоматизированных систем; -Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Виртуальные сети
Уметь:	Создавать виртуальные сети для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; -Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности.	
Владеть:	Навыками настройки сетевого оборудования с учетом требований информационной безопасности для эффективного применения информационно-технологических ресурсов автоматизированной системы; -Навыками развертывания виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы.	
Знать:	методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	Методы мониторинга информационной безопасности АС
Уметь:	выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	
Владеть:	навыками определения возможных векторов атаки на автоматизированную систему;	
Знать:	методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;	Научно-исследовательская работа
Уметь:	выполнять работы по оптимизации схем управления автоматизированной системой;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;	
Владеть:	навыками определения возможных векторов атаки на автоматизированную систему;	
Знать:	– основные понятия предметной области построения систем организационного управления – принципы построения и функционирования, примеры реализаций систем организационного управления; – основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы – основные информационные технологии, используемые в автоматизированных системах; – нормативные правовые акты в области защиты информации – возможности, классификацию и область применения макрообработки;	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь:	– применять при решении прикладных управленческих задач современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления – моделировать потоки информации, документооборот и бизнес-процессы, выполняемые в экономических системах с использованием средств Case-технологии и осуществлять их оценивание – разрабатывать техническую документацию для систем организационного управления – готовить научно-технические отчеты, обзоры, публикации по теме предметной области	
Владеть:	– навыками разработки технической документации для систем организационного управления – навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области – основами моделирования потоков информации, документооборота и бизнес-процессов в системах организационного управления	
Знать:	– основные понятия предметной области построения систем организационного управления – принципы построения и функционирования, примеры реализаций систем организационного управления; – основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы – основные информационные технологии, используемые в автоматизированных системах;	Производственная-преддипломная практика

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– нормативные правовые акты в области защиты информации – возможности, классификацию и область применения макрообработки;	
Уметь:	– применять при решении прикладных управленческих задач современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления – моделировать потоки информации, документооборот и бизнес-процессы, выполняемые в экономических системах с использованием средств Case-технологии и осуществлять их оценивание – разрабатывать техническую документацию для систем организационного управления – готовить научно-технические отчеты, обзоры, публикации по теме предметной области	
Владеть:	– навыками разработки технической документации для систем организационного управления – навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области – основами моделирования потоков информации, документооборота и бизнес-процессов в системах организационного управления	
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций		
Знать	иметь представление об основных средствах защиты информационно-технологических ресурсов автоматизированной системы; критерии защищенности ОС и сети ЭВМ; средства защиты сетей ЭВМ; о современных средствах защиты информационно-технологических ресурсов автоматизированной системы; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	Безопасность операционных систем
Уметь	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; проводить мониторинг угроз безопасности компьютерных сетей, обеспечивать защиту сетевых подключений средствами операционной системы;	
Владеть	профессиональной терминологией в области информационной безопасности; навыками работы с конкретными программными и аппаратными продуктами средств	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	телекоммуникаций, удаленного доступа и сетевыми ОС; навыками конфигурирования средств защиты информации; навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;	
Знать	Принципы работы баз данных. Основные средства обеспечения безопасности данных. Принципы администрирования баз данных. Средства обеспечения безопасности данных. Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных.	Безопасность систем баз данных
Уметь	Анализировать работоспособность базы данных. Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. Самостоятельно применять средства обеспечения безопасности данных. Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций. Организовывать безопасность систем баз данных.	
Владеть	Основными средствами обеспечения безопасности данных. Навыками работы с нормативными документами по администрированию баз данных. Средствами обеспечения безопасности данных. Навыками разработки и администрирования базы данных. Навыками организации безопасности систем баз данных. Средствами обеспечения безопасности данных и АИС.	
Знать	-требования к организационным и техническим мерам для обеспечения безопасности значимых объектов КИИ; - основные принципы организации государственного контроля состояния защищенности значимых объектов КИИ; - процедуру категорирования объектов КИИ; - требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования;	Обеспечение информационной безопасности критической информационной инфраструктурой
Уметь	- осуществлять выбор СЗИ с учетом совместимости с применяемым на значимом объекте	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	КИИ ПО и категорированием значимого объекта КИИ; - определять СЗИ для реализации технических мер обеспечения безопасности информации в рамках системы безопасности значимого объекта КИИ;	
Владеть	- навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ; - навыками разработки организационно-распорядительными документов по безопасности значимых объектов КИИ; - навыками проведения работ по контролю состояния безопасности объектов КИИ;	
Знать	- иметь представление об основных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - средства защиты сетей ЭВМ; о современных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности компьютерных сетей, обеспечивать защиту сетевых подключений средствами операционной системы;	
Владеть	- профессиональной терминологией в области информационной безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования средств защиты информации; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;	
Знать	- иметь представление об основных средствах защиты информационно-	Производственная-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - средства защиты сетей ЭВМ; о современных средствах защиты информационно-технологических ресурсов автоматизированной системы; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows	преддипломная практика
Уметь	- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; - проводить мониторинг угроз безопасности компьютерных сетей, обеспечивать защиту сетевых подключений средствами операционной системы;	
Владеть	- профессиональной терминологией в области информационной безопасности; - навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС; - навыками конфигурирования средств защиты информации; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;	
ПК-26 - способностью администрировать подсистему информационной безопасности автоматизированной системы.		
Знать	– Основные принципы работы системы информационной безопасности автоматизированной системы; – Основные принципы работы всех подсистем системы информационной безопасности автоматизированной системы; – Принципы администрирования системы информационной безопасности автоматизированной системы.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Настраивать систему информационной безопасности автоматизированной системы; – Настраивать подсистемы системы информационной безопасности автоматизированной	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	системы; – Самостоятельно администрировать систему информационной безопасности автоматизированной системы.	
Владеть	– Навыками работы с системой информационной безопасности автоматизированной системы; – Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; – Навыками администрирования системы информационной безопасности автоматизированной системы.	
Знать	– Основные принципы работы системы информационной безопасности автоматизированной системы; – Основные принципы работы всех подсистем системы информационной безопасности автоматизированной системы; – Принципы администрирования системы информационной безопасности автоматизированной системы.	Производственная-преддипломная практика
Уметь	– Настраивать систему информационной безопасности автоматизированной системы; – Настраивать подсистемы системы информационной безопасности автоматизированной системы; – Самостоятельно администрировать систему информационной безопасности автоматизированной системы.	
Владеть	– Навыками работы с системой информационной безопасности автоматизированной системы; – Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; – Навыками администрирования системы информационной безопасности автоматизированной системы.	
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы		
Знать	Принципы построения современных защищенных распределенных АС. Способы разработки политики безопасности распределенных ИС. Нормативные документы по стандартизации и сертификации программной защиты. Способы управления разработкой политики безопасности распределенных ИС. Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.	Информационная безопасность распределенных информационных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	Разрабатывать частные политики безопасности распределенных ИС. Проводить мониторинг и аудит защищенности информационно- технологических ресурсов распределенных ИС. Руководить разработкой и реализацией частных политики безопасности РИС. Осуществлять мониторинг и аудит безопасности АС.	
Владеть	Методиками анализа политики безопасности РИС. Методиками разработки политики безопасности РИС. Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. Методиками руководства разработкой политики безопасности РИС. Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС	
Знать	– способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ; – Способы разработки политики безопасности распределенных ИС. – Нормативные документы по стандартизации и сертификации программной защиты. – Способы управления разработкой политики безопасности распределенных ИС. – Методы и средства анализа достаточности мер по обеспечению ИБ ПО	Защита программного обеспечения
Уметь	– Разрабатывать частные политики безопасности распределенных ИС. – Проводить мониторинг и аудит защищенности ПО – Руководить разработкой и реализацией частных политики безопасности.	
Владеть	– Методиками анализа политики безопасности. – Методиками разработки политики безопасности. – Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО	
Знать	– Принципы построения современных защищенных распределенных АС. – Способы разработки политики безопасности распределенных ИС. – Нормативные документы по стандартизации и сертификации программной защиты. – Способы управления разработкой политики безопасности распределенных ИС. – Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.	Производственная-практика по получению профессиональных умений и опыта профессиональной

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь	– Разрабатывать частные политики безопасности распределенных ИС. – Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС. – Руководить разработкой и реализацией частных политики безопасности РИС. – Осуществлять мониторинг и аудит безопасности АС.	деятельности
Владеть	– Методиками анализа политики безопасности РИС. – Методиками разработки политики безопасности РИС. – Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. – Методиками руководства разработкой политики безопасности РИС. – Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.	
Знать	– Принципы построения современных защищенных распределенных АС. – Способы разработки политики безопасности распределенных ИС. – Нормативные документы по стандартизации и сертификации программной защиты. – Способы управления разработкой политики безопасности распределенных ИС. – Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.	Производственная-преддипломная практика
Уметь	– Разрабатывать частные политики безопасности распределенных ИС. – Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС. – Руководить разработкой и реализацией частных политики безопасности РИС. – Осуществлять мониторинг и аудит безопасности АС.	
Владеть	– Методиками анализа политики безопасности РИС. – Методиками разработки политики безопасности РИС. – Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС. – Методиками руководства разработкой политики безопасности РИС.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.	
ПК-28 способностью управлять информационной безопасностью автоматизированной системы		
Знать	основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.	Управление информационной безопасностью
Уметь	разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследоватьинциденты ИБ.	
Владеть	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ.	
Знать	-нормативные акты, используемые при разработке политики информационной безопасностью организации; – основные критерии оценки защищенности систем электронного документооборота, источники угроз методические рекомендации отраслевых регуляторов по обеспечению информационной безопасности	Информационная безопасность систем организационного управления
Уметь:	- проводить сбор и анализ данных о состоянии защиты информации в организации; оценку рисков ИБ; применять государственные стандарты и методические рекомендации для построения СЗИ организации разрабатывать политики информационной безопасности для систем электронного документооборота	
Владеть:	- навыками разработки политик информационной безопасности для систем электронного документооборота -методами моделирования потоков информации, документооборота АИС - навыками анализа данных о состоянии систем защиты информации в организации; оценки информационных оценки рисков;	
Знать	- отечественные и международные стандарты по информационной безопасности; - требования в области ИБ для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ)	Системы управления информационной безопасностью

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Уметь:	- разрабатывать техническое задание на проектирование СУИБ с учетом выявленных рисков ИБ - выбирать и анализировать технические решения для СУИБ;	
Владеть:	- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям международных стандартов; - навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям стандартов и законодательства РФ	
Знать	- Принципы получения OSINT информации.	Анализ безопасности информационных технологий
Уметь:	- Выполнять тестирование автоматизированной системы с целью получения OSINT информации.	
Владеть:	- Навыками формирования отчета о текущем уровни безопасности автоматизированной системы	
Знать	-нормативные акты, используемые при разработке политики информационной безопасностью организации; – основные критерии оценки защищенности систем электронного документооборота, источники угроз методические рекомендации отраслевых регуляторов по обеспечению информационной безопасности	Защита электронного документооборота
Уметь:	- проводить сбор и анализ данных о состоянии защиты информации в организации; оценку рисков ИБ; применять государственные стандарты и методические рекомендации для построения СЗИ организации разрабатывать политики информационной безопасности для систем электронного документооборота	
Владеть:	- навыками разработки политик информационной безопасности для систем электронного документооборота -методами моделирования потоков информации, документооборота АИС - навыками анализа данных о состоянии систем защиты информации в организации; оценки	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	информационных оценки рисков;	
Знать	- основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ.	
Владеть	- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ.	
Знать	- основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.	Производственная-преддипломная практика
Уметь	- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ.	
Владеть	- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ.	
ПРОФЕССИОНАЛЬНО-СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ		
ПСК-7.1 – способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах		
Знать	нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. Порядок разработки модели угроз	Моделирование угроз информационной безопасности
Уметь	оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные ресурсы автоматизированных систем; анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации.	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
Владеть	методами выявления угроз безопасности информации в автоматизированных системах; методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе	
Знать	- нормативные правовые акты, стандарты и руководящие документы в области защиты информации; - порядок разработки модели угроз - виды нарушителей информационной безопасности	Защита информационно-технологических ресурсов автоматизированных систем
Уметь	- определять подлежащие защите информационно-технологические ресурсы автоматизированных систем; - классифицировать и оценивать угрозы безопасности информации; - оценивать потенциал нарушителя информационной безопасности	
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.	
Знать	─ Основные понятия математического анализа, дифференциальной геометрии, численные методы оптимизации	Основы теории оптимизации
Уметь	─ Самостоятельно расширять математические знания и проводить анализ прикладных задач за счет получения дополнительной информации в условиях недостающей информации; ─ Реализовать основные алгоритмы оптимизации средствами программного обеспечения и вычислительной техники; ─ Разрабатывать алгоритмы численного решения задач оптимизации	
Владеть	Основными методами оптимизации; ─ Методами оптимизации средствами вычислительной техники; ─ Навыками реализации задач оптимизации посредством программного обеспечения общего назначения и методо-ориентированного программного обеспечения	
Знать	─ Основные принципы и схемы автоматического управления; ─ Основные требования нормативно-правовой базы в области защиты информации; ─ Основные уязвимости защищенных компьютерных систем; ─ Модели безопасности компьютерных систем; ─ Методы проведения расследования компьютерных преступлений, правонарушений и	Математическое моделирование распределенных систем

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	инцидентов; – Математические методы для анализа общих свойств распределенных систем.	
Уметь	Проводить теоретические исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы; – Применять нормативно-правовые документы в области защиты информации; – Проводить теоретические и экспериментальные исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы; – Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; – Применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований; – Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	
Владеть	Навыками выявления, исследования функциональных свойств и состояния программного обеспечения; – Навыками применения математических методов для анализа общих свойств линейных распределенных систем; – Приемами разработки математических моделей систем с распределенными параметрами; – Навыками анализа и оценки угрозы информационной безопасности объекта; – Навыками исследования алгоритма программного продукта, типов поддерживаемых аппаратных платформ; – Приемами разработки математических моделей систем с распределенными параметрами.	
Знать	Основные положения методики моделирования угроз безопасности информации Основные положения базовой модели угроз безопасности ПДн при их обработке в ИС ПДн	Информационная безопасность распределенных информационных систем
Уметь	Применять методику моделирования угроз безопасности информации для разработки частных моделей угроз и нарушителя Применять базовую модель угроз безопасности ПДн для разработки частных моделей угроз и нарушителя ИС ПДн	
Владеть	Навыками классификации угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных Навыками разработки частых моделей угроз безопасности информации	
Знать	− цели и задачи моделирования систем и процессов защиты информации; этапы	Научно-

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	моделирования и виды моделей систем и процессов защиты информации;- способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - различные информационные технологии, используемые в моделировании процессов защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем	исследовательская работа
Уметь	- обосновать выбор подходящего метода и привести алгоритм решения задачи; - формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения - применять новые технологии проектирования и анализа систем - проводить мониторинг угроз безопасности информационных систем	
Владеть	- приемами исследования проблем моделирования процессов защиты информации, возникающих в различных сферах человеческой деятельности - навыками решения моделирования процессов защиты информации - навыками проектирования информационных структур - навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; – навыками анализа основных узлов и устройств современных автоматизированных систем	
Знать	– Нормативные правовые акты в области защиты информации – Национальные, межгосударственные и международные стандарты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации – Выявление угроз безопасности информации в автоматизированных системах	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Оценивать информационные риски в автоматизированных системах – Обнаруживать нарушения правил разграничения доступа	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Классифицировать и оценивать угрозы безопасности информации – Определять подлежащие защите информационные ресурсы автоматизированных систем – Анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	
Владеть	– методами выявления угроз безопасности информации в автоматизированных системах – методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе	
Знать	– Нормативные правовые акты в области защиты информации – Национальные, межгосударственные и международные стандарты в области защиты информации – Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации – Выявление угроз безопасности информации в автоматизированных системах	Производственная-преддипломная практика
Уметь	– Оценивать информационные риски в автоматизированных системах – Обнаруживать нарушения правил разграничения доступа – Классифицировать и оценивать угрозы безопасности информации – Определять подлежащие защите информационные ресурсы автоматизированных систем – Анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	
Владеть	– методами выявления угроз безопасности информации в автоматизированных системах – методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе	
ПСК-7.2 –пособностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах		
Знать	Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах	Анализ рисков информационной безопасности
Уметь	- оценивать информационные риски в автоматизированных системах; - выполнять анализ рисков информационной безопасности в распределенных информационных системах; -	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.	
Владеть	методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем.	
Знать	- архитектуру безопасности Интернета вещей; - угрозы безопасности IoT-систем; - уязвимости информационных систем, содержащих IoT-устройства	Безопасность Интернета вещей
Уметь	- разрабатывать, руководить разработкой политики безопасности информационных систем, содержащих IoT-устройства;	
Владеть	- навыками проектирования защищенных IoT-систем.	
Знать	Ключевые процессы менеджмента ИБ Требования нормативно-правовых документов, регламентирующих систему менеджмента информационной безопасности (СМИБ)	Управление информационной безопасностью
Уметь	Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации Определять цели применения мер и средств контроля и управления для обработки рисков	
Владеть	Навыками выбора необходимых мер и средств контроля и управления ИБ Навыками определения способов измерения результативности выбранных мер управления ИБ	
Знать	– о политиках безопасности и мерах защиты в распределённых приложениях – способы обеспечения информационной безопасности систем организационного управления – Методы и средства определения технологической безопасности функционирования распределенной информационной системы – методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– формулировать основные требования к методам и средствам защиты информации в	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	защищённых распределённых приложениях – Оценивать информационные риски в автоматизированных системах – выполнять анализ рисков информационной безопасности в распределенных информационных системах – Анализировать и оценивать угрозы информационной безопасности объекта выполнять анализ рисков информационной безопасности в распределенных информационных системах	
Владеть	– методиками проведения анализа рисков информационной безопасности распределенных информационных систем – Методами оценки информационных рисков – Навыками разработки политики информационной безопасности автоматизированных систем	
Знать	– о политиках безопасности и мерах защиты в распределённых приложениях – способы обеспечения информационной безопасности систем организационного управления – Методы и средства определения технологической безопасности функционирования распределенной информационной системы – методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях	Производственная-преддипломнаяпрактика
Уметь	– формулировать основные требования к методам и средствам защиты информации в защищённых распределённых приложениях – Оценивать информационные риски в автоматизированных системах – выполнять анализ рисков информационной безопасности в распределенных информационных системах – Анализировать и оценивать угрозы информационной безопасности объекта выполнять анализ рисков информационной безопасности в распределенных информационных системах	
Владеть	– методиками проведения анализа рисков информационной безопасности распределенных информационных систем	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	– Методами оценки информационных рисков – Навыками разработки политики информационной безопасности автоматизированных систем	
ПСК-7.3. Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем		
Знать:	способы получения информации о внутренней структуре исследуемой распределенной системе; -наиболее распространённые точки для несанкционированного входа в распределенную систему;	Методы мониторинга информационной безопасности АС
Уметь:	проводить анализ уязвимостей распределённой системы; - получать несанкционированный доступ к ресурсам распределенной системы	
Владеть:	навыками противодействия внешним атакам на распределенную информационную сеть;	
Знать	― Источники и классификацию угроз информационной безопасности; ― Основные принципы построения систем защиты информации; ― Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	Аттестация АИС
Уметь:	― Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; ― Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; ― Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.	
Владеть:	― Методами выявления угроз информационной безопасности автоматизированных систем; ― Методами аудита уровня защищенности АИС.	
Знать	Принципы организации распределенных корпоративных ИС. Основные этапы аудита информационной безопасности. Основные мероприятия при проведении аудита защищенности ИС	Информационная безопасность распределенных информационных систем
Уметь:	Определять порядок организации информационного обмена между структурными подразделениями Обследовать системы на предмет наличия уязвимостей	
Владеть:	Методами оценки соблюдения требований стандартов и законов, на соответствие которым проводится аудит	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	Навыками проведения инструментального анализа защищенности (оценка достаточности имеющихся и используемых на предприятии программных и технических СЗИ и полноты их использования)	
Знать	– Источники и классификацию угроз информационной безопасности; – Основные принципы построения систем защиты информации; – Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	– Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; – Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.	
Владеть	– Методами выявления угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	
Знать:	– Источники и классификацию угроз информационной безопасности; – Основные принципы построения систем защиты информации; – Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.	Производственная-преддипломная практика
Уметь:	– Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; – Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.	
Владеть:	– Методами выявления угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита угроз информационной безопасности автоматизированных систем; – Методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	
ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах		
Знать	принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных;	Информационные технологии. Базы

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- последовательность и содержание этапов проектирования баз данных	данных
Уметь	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создаватьобъектыбазыданных;	
Владеть	методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	
Знать	Последовательность и содержание этапов построения виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах; -Основы удаленного администрирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.	Виртуальные сети
Уметь	Создавать и администрировать виртуальные локальные сети и виртуальные частные сети, а также специализированные виртуальные сети в облачных сетевых структурах; - Реализовывать политику безопасности виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах; - Пользоваться профессиональными и нестандартными (в т.ч. собственной разработки) сетевыми средствами виртуальных сетей для обмена данными, в том числе с использованием глобальной информационной сети Интернет.	
Владеть	Навыками обеспечения безопасности информации с помощью стандартных сетевых средств обмена информацией в виртуальных локальных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах; - Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, авторизации, аутентификации и аудита), виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению информационной безопасности.	
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных	Защита программного

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;	обеспечения
Уметь	- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области; - выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;	
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	
Знать	- основы администрирования в операционных системах семейств UNIX и Windows; - средства и службы удаленного управления и администрирования ОС; - модели разделения администрирования операционных систем семейств UNIX и Windows;	Безопасность операционных систем
Уметь	-выполнять настройку служб терминала; -создавать и выполнять настройку доменов, групп и учетный записей пользователей; -выполнять настройку и удаленное администрирование файлового сервера для ОС семейств UNIX и Windows;	
Владеть	- Навыками удаленного администрирования ОС семейств UNIX и Windows; -Навыками настройки и управления службами терминала; -Навыками использования командной строки для настройки и проведения удаленного администрирования ОС семейств UNIX и Windows	
Знать	- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; - основные модели данных, физическую организацию баз данных; - последовательность и содержание этапов проектирования баз данных;	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; - выделять сущности и связи предметной области;	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	- выполнять запросы к базе данных; - нормализовывать отношения при проектировании реляционной базы данных; - создавать объекты базы данных;	
Владеть	- методиками безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД.	
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении		
Знать	- Классификацию уязвимостей; - Принципы систематизации уязвимостей.	Анализ безопасности информационных технологий
Уметь	- Выполнять сканирование автоматизирование системы с цель выявления уязвимостей безопасности ИТ.	
Владеть	- Навыками исследования уязвимостей автоматизированной системы.	
Знать	– принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности	Информационная безопасность систем организационного управления
Уметь	-выявлять особенности и формировать требования к системе организации коллективной работы с информационными ресурсами СЭД -формировать комплекс мер по защите информации с учетом соответствия нормативным документам, технической реализуемости и экономической целесообразности;	
Владеть	-навыками администрирования систем электронного документооборота -навыками настройки систем предотвращения утечек информации	
Знать	– принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности	Защита электронного документооборота
Уметь	-выявлять особенности и формировать требования к системе организации коллективной работы с информационными ресурсами СЭД -формировать комплекс мер по защите информации с учетом соответствия нормативным	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	документам, технической реализуемости и экономической целесообразности;	
Владеть	-навыками администрирования систем электронного документооборота -навыками настройки систем предотвращения утечек информации	
Знать	Этапы построения и использования СМИБ Семейство стандартов ISO/IEC 27000	Управление информационной безопасностью
Уметь	Оценивать уровень знаний сотрудников в области ИБ Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ Выявлять возможности улучшения СМИБ	
Владеть	Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ	
Знать	- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации -основные вопросы организации организационного управления, виды и признаки классификации, основные требования стандартизации и унификации документов, способствующие повышению эффективности функционирования системы управления организацией -современные технологии и основные характеристики систем организационного управления, представленных на российском рынке -методы и средства проектирования систем организационного управления - методы и средства моделирования и оптимизации документооборота и бизнес-процессов автоматизации контроля исполнения и анализа их с целью дальнейшего совершенствования -организационные меры по защите информации	Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности
Уметь	-выбирать методы и подходы к проектированию СЭДО на предприятии; -разрабатывать постановку задачи и выбирать методы и средства построения системы преобразования бумажных документов в электронную форму, ввода их в электронный архив, организации хранения и поиска документов, формирования отчетов о работе системы -выявлять особенности и формировать требования к системе организации коллективной работы с документами в режиме совместного доступа и передачи их на исполнение по	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	электронной почте или по локальной сети; -выполнять настройки систем планирования маршрутов передвижения документов и контролировать их исполнение	
Владеть	-навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области -основами моделирования потоков информации, документооборота и бизнес-процессов -навыками администрирования систем организационного управления	
Знать	- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации -основные вопросы организации организационного управления, виды и признаки классификации, основные требования стандартизации и унификации документов, способствующие повышению эффективности функционирования системы управления организацией -современные технологии и основные характеристики систем организационного управления, представленных на российском рынке -методы и средства проектирования систем организационного управления - методы и средства моделирования и оптимизации документооборота и бизнес-процессов автоматизации контроля исполнения и анализа их с целью дальнейшего совершенствования -организационные меры по защите информации	Производственная-преддипломная практика
Уметь	-выбирать методы и подходы к проектированию СЭДО на предприятии; -разрабатывать постановку задачи и выбирать методы и средства построения системы преобразования бумажных документов в электронную форму, ввода их в электронный архив, организации хранения и поиска документов, формирования отчетов о работе системы -выявлять особенности и формировать требования к системе организации коллективной работы с документами в режиме совместного доступа и передачи их на исполнение по электронной почте или по локальной сети; -выполнять настройки систем планирования маршрутов передвижения документов и	

Структурный элемент компетенции	*Планируемые результаты обучения*	*Структурный элемент образовательной программы*
	контролировать их исполнение	
Владеть	-навыками подготовки научно-технических отчетов, обзоров, публикаций по теме предметной области -основами моделирования потоков информации, документооборота и бизнес-процессов -навыками администрирования систем организационного управления	