



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 № 10 от « 25 » октября 2017 г.

Ректор МГТУ им. Г.И. Носова,
председатель ученого совета


В.М. Колокольников

**АННОТАЦИИ ДИСЦИПЛИН
ПО ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ
ВЫСШЕГО ОБРАЗОВАНИЯ**

Специальность

**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность (специализация) программы

**Обеспечение информационной безопасности распределенных
информационных систем**

Магнитогорск, 2017

ОП-АИБ-17

8.3 АННОТАЦИИ ДИСЦИПЛИН ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
Б1	Дисциплины (модули)	
Б1.Б	Базовая часть	
Б1.Б.01	<p>История</p> <p>1 Цели освоения дисциплины (модуля) Целями освоения дисциплины «История» являются: сформировать у студентов комплексное представление о культурно-историческом своеобразии России, ее месте в мировой и европейской цивилизации; сформировать систематизированные знания об основных закономерностях и особенностях всемирно-исторического процесса, с акцентом на изучение истории России; введение в круг исторических проблем, связанных с областью будущей профессиональной деятельности, выработка навыков получения, анализа и обобщения исторической информации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина История входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Для освоения этого курса необходимы знания (умения, навыки), сформированные в результате изучения предметов «История России», «Всеобщая история» и «Обществознание» (школьные курсы) Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Философия Правоведение</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «История» обучающийся должен обладать следующими компетенциями: 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</p> <p>Знать -Основные проблемы, периоды, тенденции и особенности исторического процесса, -Осознавать место истории России во всемирно-историческом процессе</p> <p>Уметь выражать и обосновывать свою позицию по вопросам, касающимся ценностного отношения к историческому прошлому.</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <p>Навыками межличностной и межкультурной коммуникации, основанные на уважении к историческому наследию и культурным традициям</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. История в системе социально-гуманитарных наук. Основы методологии исторической науки <ol style="list-style-type: none"> 1.1 Теория и методология исторической науки 2. Древнейшая стадия истории человечества <ol style="list-style-type: none"> 2.1 Государство и общество в Древнем мире 2.2 Древнерусское государство в IX – XII вв. 3. Средневековье как стадия исторического процесса <ol style="list-style-type: none"> 3.1 Средневековье как стадия всемирного исторического процесса. 3.2 Русские земли в период раздробленности. Борьба русских земель с иноземными захватчиками 3.3 Образование и становление русского централизованного государства в XIV – первой трети XVI вв. 4. Россия и мир в XVI-XVIII вв. <ol style="list-style-type: none"> 4.1 Раннее Новое Время: переход к индустриальному обществу 4.2 Иван Грозный: реформы и опричнина 4.3 Россия в XVII в. 4.4 Преобразования традиционного общества при Петре I 4.5 Дворцовые перевороты. Правление Екатерины II 5. Россия и мир в XIX веке. <ol style="list-style-type: none"> 5.1 Мир XVIII – XIX вв.: попытки модернизации и промышленный переворот. 5.2 Россия в первой половине XIX в. 5.3 Россия во второй половине XIX в. 6. Россия и мир в конце XIX- начале XX вв. <ol style="list-style-type: none"> 6.1 Мир в начале XX века. Первая мировая война 6.2 Первая российская революция и ее последствия. 6.3 Россия в 1917 г. 7. Россия и мир во второй половине XX века <ol style="list-style-type: none"> 7.1 Послевоенное устройство мира (1946 – 1991) 7.2 СССР в 1945-1964 гг.: послевоенное восстановление народного хозяйства и попытки реформирования 7.3 СССР в 1965 – 1991 гг. 8. Россия и мир между двумя мировыми войнами. Вторая мировая война. <ol style="list-style-type: none"> 8.1 Мир между двумя мировыми войнами. Вторая мировая война. 8.2 Социалистическая революция и становление советской власти (октябрь 1917-май 1918 гг.). Гражданская война и интервенция 8.3 Внутренняя политика СССР в 1920 – 1930-е гг. 8.4 СССР в годы Великой Отечественной войны 9. Мир на рубеже XX-XXI вв.: пути развития современной 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>цивилизации, интеграционные процессы, меж-дународные отношения</p> <p>9.1 Мировое сообщество на рубеже XX – XXI веков</p> <p>9.2 Внутренняя политика Российской Федерации (1991 – 2000-е гг.).</p> <p>10. Экзамен</p>	
Б1.Б.02	<p>Иностранный язык</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью освоения дисциплины «Иностранный язык» является: повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования; овладение студентами необходимым и достаточным уровнем иноязычной коммуникативной компетенции в устной и письменной формах для решения социально-значимых задач в различных областях бытовой, культурной, профессиональной и научной деятельности, а также для дальнейшего самообразования.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Иностранный язык входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Дисциплина «Иностранный язык» относится к базовой части образовательной программы (Б1.Б.02).</p> <p>Для изучения дисциплины необходимы знания, умения, владения, сформированные в результате изучения иностранного языка на предыдущем этапе образования.</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Иностранный язык» обучающийся должен обладать следующими компетенциями:</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 	<p><i>Общая трудоемкость дисциплины составляет 7 зачетных единиц</i></p> <p><i>252 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>коммуникативных ситуациях; разговорные формулы этикета профессионального общения, приемы структурирования научного дискурса. Уметь</p> <ul style="list-style-type: none"> - 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 перевода, его целей и условий осуществления. <p>Владеть</p> <ul style="list-style-type: none"> - 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). <p>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</p> <p>Знать</p> <p>основные приемы и методы, связанные с поиском, изучением, обобщением и систематизацией научно-технической информации</p> <p>Уметь</p> <p>использовать основные приемы и методы для поиска, изучения, обобщения и систематизации научно-технической информации</p> <p>Владеть</p> <p>основными приемами и методами для поиска, изучения, обобщения и систематизации научно-технической информации</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Я в современном мире</p> <p>1.1 Развитие умений и навыков чтения, говорения и письма по указанной теме</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.2 Развитие умений и навыков оперирования лексическими и грамматическими структурами для обеспечения необходимой иноязычной коммуникации по указанной теме</p> <p>2. Ценности образования</p> <p>2.1 Развитие навыков чтения, говорения и письма по теме «Система высшего образования в России и странах изучаемого языка»</p> <p>2.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме</p> <p>3. История научной мысли</p> <p>3.1 Развитие умений и навыков чтения, говорения и письма по теме «Выдающиеся учёные мира» , «Величайшие изобретения человечества»</p> <p>3.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме</p> <p>4. Страна, где я живу</p> <p>4.1 Развитие умений и навыков чтения, говорения и письма по теме: «Российская Федерация: география, политическая система, культура, люди»</p> <p>5. Страны изучаемого языка</p> <p>5.1 Развитие умений и навыков чтения, говорения и письма по теме: « География, культура и традиции страны изучаемого языка» »</p> <p>5.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме</p> <p>6. Современное производство и окружающая среда</p> <p>6.1 Развитие умений и навыков чтения, говорения и письма по теме. «ММК – одно из крупнейших предприятий металлургической отрасли России и мира»; «Природные и экологические явления и изменения»; «Защита окружающей среды»</p> <p>6.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме</p> <p>7. Достижения научно-технического прогресса</p> <p>7.1 Развитие умений и навыков чтения, говорения и письма по теме: «Роль и место инновационных технологий в современном мире» ; «Информационные технологии 21-го века»</p> <p>7.2 Диагностика сформированности навыков и умений по всем видам речевой деятельности</p>	
Б1.Б.03	Философия 1 Цели освоения дисциплины (модуля)	<i>Общая трудоем</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- способствовать развитию гуманитарной культуры студента посредством его приобщения к опыту философского мышления, формирования потребности и навыков критического осмысления состояния, тенденций и перспектив развития культуры, цивилизации, общества, истории, личности.</p> <p>- предоставление необходимого минимума знаний для формирования мировоззренческих оснований научно-исследовательской деятельности;</p> <p>- сформировать представление о специфике философии как способе познания и духовного освоения мира;</p> <p>- сформировать целостное представление о процессах и явлениях, происходящих в неживой и живой природе и общественной жизни;</p> <p>- привить навыки работы с оригинальными и адаптированными философскими текстами;</p> <p>- сформировать представление о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека;</p> <p>- сформировать представление о многообразии форм человеческого знания, соотношении истины и заблуждения, знания и веры, рационального и иррационального в человеческой жизнедеятельности, особенностях функционирования знания в современном обществе;</p> <p>- сформировать представление о ценностных основаниях человеческой деятельности;</p> <p>- определить основания активной жизненной позиции, ввести в круг философских проблем, связанных с областью будущей профессиональной деятельности.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Философия входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Культурология и межкультурное взаимодействие</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Философия» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции</p> <p>Знать</p>	<p><i>кость дисциплины составляет 4 зачетных единицы</i></p> <p>144</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- основные философские категории и специфику их понимания в различных исторических типах философии и авторских подходах;</p> <p>- основные направления философии и различия философских школ в контексте истории;</p> <p>- основные направления и проблематику современной философии;</p> <p>Уметь</p> <p>- раскрывать смысл выдвигаемых идей, корректно выражать и аргументировано обосновывать положения предметной области знания;</p> <p>- представлять рассматриваемые философские проблемы в развитии;</p> <p>- сравнивать различные философские концепции по конкретной проблеме;</p> <p>- уметь отметить практическую ценность определенных философских положений и выявить основания, на которых строится философская концепция или система;</p> <p>Владеть</p> <p>- навыками работы с философскими источниками и критической литературой;</p> <p>- приемами поиска, систематизации и свободного изложения философского материала и методами сравнения философских идей, концепций и эпох;</p> <p>- способами обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации;</p> <p>- владеть навыками выражения и обоснования собственной позиции относительно современных социогуманитарных проблем и конкретных философских позиций</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1.1 Философская картина мира: концепция человека и проблема бытия</p> <p>2.1 История философии: многообразие картин материального мира. Сущность и смысл существования человека. Материальное бытие</p> <p>3.1 Идеальное бытие: сознание, мышление, язык. Гносеология: познавательные отношения человека с объективной реальностью. Методологические проблемы познания.</p> <p>4.1 Динамика общественного развития. Общество. Философская концепция культуры. Философское и нефилософское понимание материи</p>	
Б1.Б.04	<p>Экономика</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>- изучение фундаментальных закономерностей экономического развития общества, лежащих в основе всей системы экономических знаний, анализ функционирования рыночной экономики на микро и макроуровне, определение роли государственных институтов в экономике, рассмотрение теоретических концепций,</p>	<p><i>Общая трудоемкость дисциплины составляет 3</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обосновывающих механизм эффективного функционирования экономики;</p> <ul style="list-style-type: none"> - освоение навыков оценки использования ресурсов предприятия и результатов его деятельности; - формирование у студентов основ экономического мышления; - выработка способности использовать основы экономических знаний в различных сферах жизнедеятельности; - формирование компетенций, необходимых при решении профессиональных задач. <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Экономика входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>История</p> <p>Алгебра и геометрия</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>Продвижение научной продукции</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Экономика» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - ориентироваться в типовых экономических ситуациях, основных вопросах экономической политики; - использовать элементы экономического анализа в своей профессиональной деятельности; 	<p>зачетных единиц 108 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- 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.</p> <p>Владеть</p> <p>- 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, анализировать и объяснять экономические явления, события, ситуации.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Микроэкономика 1.1 Введение в экономическую теорию 1.2 История экономических учений 1.3 Законы рыночной экономики: спрос, предложение, ценообразование 1.4 Производитель и потребитель в рыночной экономике 1.5 Конкуренция: виды рыночных структур</p> <p>2. Макроэкономика 2.1 Закономерности функционирования национальной экономики 2.2 Цикличность экономического развития 2.3 Экономическая политика государства</p> <p>3. Экономика предприятия 3.1 Предприятие как хозяйствующий субъект рыночной экономики 3.2 Ресурсы предприятия 3.3 Затраты и финансовые результаты деятельности предприятия</p>	
Б1.Б.05	<p>Правоведение</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Правоведение» являются: формирование у студентов знаний для правового ориентирования в системе законодательства, определение соотношения юридического содержания норм с реальными событиями общественной жизни, изучение основополагающих правовых понятий.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Правоведение входит в базовую часть учебного плана</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>История</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>3 Компетенции обучающегося, формируемые в результате освоения</p> <p>дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Правоведение» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>Знать</p> <p>основные правовые понятия;</p> <p>основные источники права;</p> <p>принципы применения юридической ответственности</p> <p>Уметь</p> <p>ориентироваться в системе законодательства;</p> <p>определять соотношение юридического содержания норм с реальными событиями общественной жизни;</p> <p>разрабатывать документы правового характера;</p> <p>приобретать знания в области права;</p> <p>корректно выражать, аргументировано обосновывать свою юридическую позицию</p> <p>Владеть</p> <p>практическими навыками анализа и разрешения юридических ситуаций;</p> <p>практическими навыками совершения юридических действий в соответствии с законом;</p> <p>навыками составления претензий, заявлений, жалоб по факту неисполнения или ненадлежащего исполнения прав;</p> <p>способами совершенствования правовых знаний и умений путем использования возможностей информационной среды</p> <p>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</p> <p>Знать</p> <p>роль правовой информации в развитии современного общества и профессиональной деятельности;</p> <p>виды источников права</p> <p>систему законодательства Российской Федерации</p> <p>Уметь</p> <p>находить и анализировать правовую информацию;</p>	<p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>использовать правовую информацию при решении конкретных жизненных ситуаций Владеть практическими навыками работы со справочно-поисковыми системами Консультант Плюс и Гарант Дисциплина включает в себя следующие разделы: 1. Раздел Основы государства и права 1.1 Тема Государство: понятие, признаки, формы. Основы конституционного строя Российской Федерации 1.2 Тема Право: понятие, источники. Правонарушение и юридическая ответственность. Значение законности и правопорядка в современном обществе. Борьба с коррупцией 2. Раздел Основы частного права 2.1 Тема Основы гражданского права 2.2 Тема Основы семейного права 2.3 Тема Основы трудового права 3. Раздел Основы публичного права 3.1 Тема Основы административного права 3.2 Тема Основы уголовного права 3.3 Тема Основы экологического права 4. Раздел Особенности правового регулирования будущей профессиональной деятельности 4.1 Тема Особенности правового регулирования будущей профессиональной деятельности</p>	
Б1.Б.06	<p>Культурология и межкультурное взаимодействие 1 Цели освоения дисциплины (модуля) Целями освоения дисциплины являются: – формирование, закрепление и расширение базовых знаний о культурологии как науке и о культурном взаимодействии как предмете культурологии; об основных разделах современного культурологического знания и о проблемах и методах их исследования; – получение знаний об основных формах и закономерностях мирового процесса развития культуры в ее общих и единичных характеристиках, выработке навыков самостоятельного овладения миром ценностей культуры для совершенствования своей личности и профессионального мастерства. 2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Культурология и межкультурное взаимодействие входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Иностранный язык</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>История</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Культурология и межкультурное взаимодействие» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p> <p>Знать</p> <ul style="list-style-type: none"> – 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. <p>Уметь</p> <ul style="list-style-type: none"> – 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. <p>Владеть</p> <ul style="list-style-type: none"> – навыками коммуникаций в профессиональной сфере, критики и самокритики, терпимостью; – навыками культурного сотрудничества, ведения переговоров и разрешения конфликтов; – навыками толерантного восприятия социальных и культурных различий. <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> – 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, 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>многовариантность культурного процесса.</p> <p>Уметь</p> <ul style="list-style-type: none"> – 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. <p>Владеть</p> <ul style="list-style-type: none"> – навыками межкультурного взаимодействия; – критического восприятия культурно значимой информации; – навыками социокультурного анализа современной действительности; – навыками социального взаимодействия, сотрудничества в позициях расовой, национальной, религиозной терпимости. <p>ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции</p> <p>Знать</p> <ul style="list-style-type: none"> -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 <p>Уметь</p> <ul style="list-style-type: none"> -выстраивать собственную мировоззренческую позицию на основе имеющихся культурно-философских знаний; -обосновывать собственную мировоззренческую позицию; -формировать новые взгляды и представления, основанные на существующих мировоззренческих позициях представителей различных культурных систем <p>Владеть</p> <ul style="list-style-type: none"> - 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>формирования мировоззренческой позиции</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Культурология в системе научного знания и проблема межкультурного взаимодействия</p> <p>1.1 Культурология в системе научного знания</p> <p>1.2 Культурогенез и проблема межкультурного взаимодействия</p> <p>1.3 Основные теории происхождения культуры</p> <p>2. Основные понятия культурологии</p> <p>2.1 Основные понятия культурологии</p> <p>2.2 Основные формы и типы культуры</p> <p>2.3 Культура как система знаков</p> <p>3. История культурологических учений</p> <p>3.1 Доклассический и классический периоды развития культурологии</p> <p>3.2 Развитие культурологии во второй половине XIX – XX веках</p> <p>3.3 Типология культур</p>	
Б1.Б.07	<p>Технология командообразования и саморазвития</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Технология командообразования и саморазвития» являются: формирование у студентов универсальных, общепрофессиональных и профессио-нальных компетенций, позволяющих им успешно решать весь спектр задач, связанных с созданием и функционированием команд в организациях, а также отчетливо выраженного индивидуального взгляда на проблему создания и функционирования управленческой команды, понимания ее сути как социально-психологического феномена.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Технология командообразования и саморазвития входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>История</p> <p>Введение в специальность</p> <p>Культурология и межкультурное взаимодействие</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Правоведение</p> <p>Философия</p> <p>Экономика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i></p> <p>108</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Технология командообразования и саморазвития» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p> <p>Знать принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия</p> <p>Уметь находить организационно - управленческие решения в нестандартных ситуациях</p> <p>Владеть умением находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность</p> <p>ОК-8 способностью к самоорганизации и самообразованию</p> <p>Знать способы самоорганизации и развития своего интеллектуального, культурного, духовного, нравственного, физического и профессионального уровня</p> <p>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</p> <p>Владеть технологиями организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Теоретические основы командообразования <ol style="list-style-type: none"> 1.1 Команда как вид групп высшего уровня развития 1.2 Формирование команды 2. Внутриккомандные процессы и отношения <ol style="list-style-type: none"> 2.1 Распределение ролей и особенности работы в команде 2.2 Коммуникации в команде 2.3 Управление конфликтами в командах 2.4 Управление взаимоотношениями в команде 3. Саморазвитие членов команды <ol style="list-style-type: none"> 3.1 Жизненный путь личности и саморазвитие. Индивидуальный 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	коучинг	
Б1.Б.08	<p>Безопасность жизнедеятельности</p> <p>1 Цели освоения дисциплины (модуля) Целью освоения дисциплины «Безопасность жизнедеятельности» является формирование у студентов знаний и навыков, способных обеспечить решение задач в области создания безопасных условий деятельности при проектировании и использовании техники и технологических процессов, а также при прогнозировании и ликвидации последствий стихийных бедствий, аварий и катастроф</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина «Безопасность жизнедеятельности» входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Физика Информатика Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Производственная-преддипломная практика Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Безопасность жизнедеятельности» обучающийся должен обладать следующими компетенциями: 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 Уметь - выделять основные опасности среды обитания человека; - оценивать риск их реализации Владеть - основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Дисциплина включает в себя следующие разделы:</p> <p>Раздел 1. 1.1 Теоретические основы безопасного и безвредного взаимодействия человека со средой обитания. Первая доврачебная помощь</p> <p>Раздел 2. 2.1 Формирование опасностей в производственной среде. Идентификация вредных и опасных факторов технических систем</p> <p>Раздел 3. 3.1 Технические методы и средства повышения безопасности и экологичности производственных систем</p> <p>Раздел 4. 4.1 Прогнозирование и ликвидация чрезвычайных ситуаций</p> <p>Раздел 5. 5.1 Правовые и организационные основы безопасности жизнедеятельности. Управление безопасностью жизнедеятельности</p>	
Б1.Б.09	<p>Физика</p> <p>1 Цели освоения дисциплины (модуля) Целью освоения дисциплины «Физика» является формирование у обучающихся способности применять основные законы классической и современной физики для анализа физических явлений и процессов, их формализации и решения задач с помощью соответствующего физико-математического аппарата, а также умения работать с оборудованием, обрабатывать и представлять данные измерений и делать обоснованные выводы.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Физика входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик: «Физика», «Математика», «Информатика» на базе среднего (полного) общего образования. Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Основы радиотехники Физические основы передачи информации Электроника и схемотехника Техническая защита информации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p>	<p><i>Общая трудоемкость дисциплины составляет 15 зачетных единиц 540 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>В результате освоения дисциплины (модуля) «Физика» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать</p> <ul style="list-style-type: none"> – основные законы физики, границы применимости этих законов и их связь с явлениями и процессами, происходящими в природе; – методы анализа физических процессов и явлений; – физико-математический аппарат, используемый для описания физических закономерностей <p>Уметь</p> <p>применять физические законы и физико-математический аппарат для формализации описания физических явлений и процессов и решения задач в рамках физики и смежных дисциплин</p> <p>Владеть</p> <p>опытом анализа происходящих физических явлений и процессов и решения физических задач</p> <p>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Знать</p> <p>методы и подходы к экспериментальному исследованию и моделированию, применяемые в физике и распространяющиеся на другие области знаний</p> <p>Уметь</p> <ul style="list-style-type: none"> – пользоваться современной аппаратурой для проведения физического эксперимента; – использовать физические модели для описания реальных процессов, с помощью приборов измерять физические величины, производить обработку экспериментальных данных и анализировать полученные результаты <p>Владеть</p> <ul style="list-style-type: none"> – навыками работы с измерительными приборами и оборудованием; – методами проведения физических измерений, расчета величин и анализа полученных данных <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Механика <ol style="list-style-type: none"> 1.1 Кинематика поступательного и вращательного движения 1.2 Динамика поступательного и вращательного движения 1.3 Законы сохранения в механике 1.4 Релятивистская механика 1.5 Механические колебания и волн 2. Молекулярная физика и термодинамика 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>2.1 Молекулярно-кинетическая теория и основы статистической физики</p> <p>2.2 Термодинамика</p> <p>3. Электромагнетизм</p> <p>3.1 Электростатика</p> <p>3.2 Постоянный ток</p> <p>3.3 Магнитостатика</p> <p>3.4 Электромагнитная индукция. Электромагнитные колебания. Переменный ток</p> <p>4. Волновая оптика</p> <p>4.1 Электромагнитное поле. Электромагнитные волны. Волновая природа света.</p> <p>4.2 Взаимодействие света с веществом. Поляризация света</p> <p>4.3 Интерференция света</p> <p>4.4 Дифракция света</p> <p>5. Квантовая оптика</p> <p>5.1 Квантовая оптика. Экспериментальное подтверждение квантовой природы света</p> <p>6. Квантовая физика и физика атома</p> <p>6.1 Элементы квантовой механики</p> <p>6.2 Физика атома</p> <p>6.3 Квантовая статистика. Элементы физики твердого тела.</p> <p>7. Физика ядра и элементарных частиц</p> <p>7.1 Физика атомного ядра. Радиоактивность</p> <p>7.2 Физика элементарных частиц и современная картина мира</p>	
Б1.Б.10	<p>Основы управленческой деятельности</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины (модуля) «Основы управленческой деятельности» является формирование способности к коммуникации для решения задач межличностного и межкультурного взаимодействия; навыков организации работы малых коллективов исполнителей и принятия управленческих решений в сфере профессиональной деятельности.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы подготовки специалиста</p> <p>Дисциплина «Основы управленческой деятельности» входит в базовую часть блока 1 образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин «Технология командообразования и саморазвития», «Экономика».</p>	<p><i>Общая трудоемкость дисциплины составляет 2 зачетных единицы 72 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы при подготовке и защите выпускной квалификационной работы.</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Основы управленческой деятельности» обучающийся должен обладать следующими компетенциями:</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> – понятие и содержание управленческой деятельности <p>Уметь</p> <ul style="list-style-type: none"> – анализировать внешнюю и внутреннюю среду организации как объекта управленческой деятельности <p>Владеть</p> <ul style="list-style-type: none"> – основными навыками управленческой деятельности: планирования, организации, мотивации, контроля и коммуникаций <p>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> – основы принятия управленческих решений <p>Уметь</p> <ul style="list-style-type: none"> – организовывать работу малых коллективов исполнителей <p>Владеть</p> <ul style="list-style-type: none"> – навыками управления поведением человека в организации <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Понятие и содержание управления 2. Эволюция теории и практики управления. Школы научного управления 3. Организация как объект управления. Организационно-правовые формы субъектов экономики 4. Организационные структуры управления. Типология организационных структур 5. Управление как процесс. Планирование, организация, мотивация, контроль как функции управления 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	6. Принятие управленческих решений 7. Управление коммуникациями 8. Руководство и лидерство. Стили лидерства 9. Управление поведением человека в организации. Формы власти и влияния.	
Б1.Б.11	<p>Алгебра и геометрия</p> <p>1 Цели освоения дисциплины (модуля)</p> <ul style="list-style-type: none"> • развитие математического мышления; • формирование навыков решения геометрических задач в различных системах координат; • ознакомление с основами классической и современной алгебры; • ознакомление с различными алгебраическими структурами (полями, векторными пространствами) и их приложениями в решении различных практических задач; • обучение основным алгебраическим методам решения задач, возникающих в других математических дисциплинах и в практике; • воспитание у студентов математической и технической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для современного специалиста. <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Алгебра и геометрия входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин: «Алгебра и начала анализа», «Геометрия» в объеме программы средней школы.</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Дискретная математика Теория вероятностей, математическая статистика Математический анализ Исследование операций и теория игр Основы теории оптимизации Математическое моделирование распределенных систем Теория графов и ее приложения</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Алгебра и геометрия» обучающийся должен обладать следующими компетенциями:</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i></p> <p>108</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> - основные понятия линейной алгебры и аналитической геометрии - возможности координатного метода для исследования различных геометрических объектов - аналитические способы описания алгебраических структур и геометрических объектов <p>Уметь</p> <ul style="list-style-type: none"> - 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; - 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 <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Линейная алгебра <ol style="list-style-type: none"> 1.1 Матрицы. Определители. Системы линейных алгебраических уравнений. 1.2 Линейные пространства. Базис. Евклидовы пространства. 1.3 Линейные операторы. 1.4 Квадратичные формы. 2. Векторная алгебра <ol style="list-style-type: none"> 2.1 Векторы и операции над ними. Скалярное, векторное и 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>смешанное произведение векторов.</p> <p>3. Аналитическая геометрия</p> <p>3.1 Системы координат на плоскости. Прямая на плоскости. Кривые на плоскости.</p> <p>3.2 Кривые второго порядка: окружность, эллипс, гипербола, парабола.</p> <p>3.3 Преобразование координат: параллельный перенос, поворот. Классификация линий 2-го порядка. Приведение уравнений линий 2-го порядка к каноническому виду</p> <p>3.4 Системы координат в пространстве. Плоскость, прямая в пространстве.</p> <p>3.5 Поверхности второго порядка: цилиндрические, конические и поверхности вращения. Эллипсоид, гиперболоиды, параболоиды.</p> <p>3.6 Классификация поверхностей второго порядка. Приведение к каноническому виду общего уравнения поверхности второго порядка.</p>	
Б1.Б.12	<p>Математический анализ</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Цель освоения дисциплины – ознакомить обучаемых с основными понятиями и методами математического анализа, создать теоретическую и практическую базу подготовки специалистов к деятельности, связанной с проектированием, разработкой и применением электронной аппаратуры для обеспечения безопасности автоматизированных систем.</p> <p>Задача дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Математический анализ входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Алгебра и геометрия</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Дискретная математика</p> <p>Теория вероятностей, математическая статистика</p> <p>Исследование операций и теория игр</p> <p>Математическая логика и теория алгоритмов</p> <p>3 Компетенции обучающегося, формируемые в результате</p>	<p><i>Общая трудоемкость дисциплины составляет 7 зачетных единиц</i></p> <p>252</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Математический анализ» обучающийся должен обладать следующими компетенциями: ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 <p>Уметь</p> <ul style="list-style-type: none"> - 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 <p>Владеть</p> <ul style="list-style-type: none"> - 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 <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Предел и непрерывность функции одной переменной 1.1 Понятие множества. Действительные числа и их свойства. Понятие окрестности точки. Понятие функции. Свойства функций 1.2 Числовые последовательности. Предел числовой последовательности. Сходимость последовательности. Ограниченные и монотонные последовательности. Простейшие свойства пределов последовательностей. Число e.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Предел функции на языке последовательностей. Бесконечно большие, бесконечно малые. Свойства пределов функций. Основные виды неопределенностей</p> <p>1.3 Непрерывность функции в точке и на множестве. Арифметические операции над непрерывными функциями. Непрерывность элементарных функций. Свойства функций, непрерывных на отрезке. Точки разрыва и их классификация</p> <p>2. Дифференциальное исчисление функции одной действительной переменной</p> <p>2.1 Задачи, приводящие к понятию производной. Определение производной функции в точке. Дифференциал, его геометрический смысл. Геометрический и механический смысл производной. Правила дифференцирования и таблица производных</p> <p>2.2 Дифференцирование неявно заданных, параметрически заданных функций. Логарифмическое дифференцирование</p> <p>2.3 Производные и дифференциалы высших порядков</p> <p>2.4 Основные теоремы дифференциального исчисления: теоремы Ферма, Ролля, Лагранжа, Коши. Формула Тейлора. Формула Тейлора. Применение производных при вычислении пределов. Правило Лопиталя</p> <p>2.5 Исследование функций с помощью дифференциального исчисления. Признаки знакопостоянства, возрастания и убывания, выпуклости и вогнутости графика функции на промежутке. Экстремумы функций. Нахождение наименьшего и наибольшего значений функции на замкнутом промежутке</p> <p>3. Интегральное исчисление функции одной действительной переменной</p> <p>3.1 Первообразная функция. Неопределенный интеграл и его основные свойства. Таблица неопределенных интегралов от основных элементарных функций</p> <p>3.2 Методы непосредственного интегрирования. Интегрирование заменой переменной и по частям</p> <p>3.3 Интегрирование рациональных дробей</p> <p>3.4 Интегрирование тригонометрических выражений. Интегрирование иррациональных выражений</p> <p>3.5 Задача вычисления площади криволинейной трапеции и другие задачи, приводящие к понятию определенного интеграла. Формула Ньютона-Лейбница. Свойства определенного интеграла. Существование первообразной непрерывной функции. Замена переменной и интегрирование по частям</p> <p>3.6 Несобственные интегралы. Признаки сходимости</p> <p>4. Дифференциальное исчисление функций нескольких переменных (ФНП)</p> <p>4.1 Предел и непрерывность ФНП. Основные свойства функций,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>непрерывных в замкнутой области</p> <p>4.2 Частные производные и производная по направлению. Дифференцируемые функции. Касательная плоскость и нормаль к поверхности. Геометрический смысл дифференциала. Признак дифференцируемости</p> <p>4.3 Производная сложной функции. Частные производные и дифференциалы высших порядков. Дифференцирование неявно заданных функций</p> <p>4.4 Экстремумы ФНП</p> <p>5. Интегральное исчисление функций нескольких переменных (ФНП)</p> <p>5.1 Двойной интеграл и его основные свойства. Сведение двойного интеграла к повторному интегралу. Теорема о среднем значении. Замена переменных, переход в двойном интеграле к полярным координатам</p> <p>5.2 Сведение тройного интеграла к повторному интегралу. Замена переменных, переход в тройном интеграле к цилиндрическим и сферическим координатам</p> <p>5.3 Геометрические и механические приложения кратных интегралов</p> <p>5.4 Криволинейные интегралы I и II рода. Вычисление и простейшие свойства криволинейных интегралов. Понятие о поверхностных интегралах</p> <p>6. Обыкновенные дифференциальные уравнения (ОДУ)</p> <p>6.1 Обыкновенные дифференциальные уравнения первого порядка. Основные определения. Частное и общее решение. Интегральные кривые. Геометрический смысл дифференциального уравнения первого порядка. Методы решения дифференциальных уравнений первого порядка</p> <p>6.2 ДУ высших порядков, допускающие понижение порядка</p> <p>6.3 Линейные дифференциальные уравнения n-го порядка. Линейное однородное уравнение. Фундаментальная система решений. Определитель Вронского. Неоднородное линейное уравнение (ЛНДУ), вид общего решения. Метод вариации произвольных постоянных. Линейное уравнение с постоянными коэффициентами. Характеристическое уравнение. Общее решение</p> <p>6.4 Методы решения систем дифференциальных уравнений (2-го порядка)</p> <p>7. Элементы теории числовых и функциональных рядов</p> <p>7.1 Понятие числового ряда. Понятие сходимости ряда. Признаки сходимости знакоположительных рядов. Знакопеременные ряды. Ряд Лейбница</p> <p>7.2 Основные понятия теории функциональных рядов. Сходимость. Равномерная сходимость функционального ряда. Непрерывность,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>дифференцируемость и интегрируемость суммы функционального ряда. Степенные ряды. Теоремы Абеля. Радиус сходимости. Непрерывность, дифференцируемость и интегрируемость суммы степенного ряда. Ряд Тейлора. Разложение в ряд Маклорена основных элементарных функций. Приложения степенных рядов 7.3 Основные задачи гармонического анализа. Ортогональные системы функций. Тригонометрическая система функций. Ряд Фурье. Признаки сходимости рядов Фурье 8. Элементы теории функций комплексной переменной (ФКП) 8.1 Комплексные числа. Операции над комплексными числами. Функции комплексной переменной 8.2 Производная. Условия Коши-Римана (Даламбера-Эйлера) дифференцируемости функций комплексной переменной. Гармонические функции и их связь с аналитическими функциями. Геометрический смысл аргумента и модуля производной. Интегралы от комплекснозначных функций действительной и комплексной переменной. Простейшие свойства. Теорема Коши. Интегральная формула Коши 8.3 Степенные ряды с комплексными членами. Ряд Тейлора. Показательная и логарифмическая функции. Тригонометрические функции. Ряд Лорана. Изолированные особые точки. Разложение функции в ряд Лорана. Элементы теории вычетов</p>	
Б1.Б.13	<p>Теория вероятностей и математическая статистика 1 Цели освоения дисциплины (модуля) Целью освоения дисциплины «Теория вероятностей и математическая статистика» является ознакомление студентов с базовыми понятиями и результатами теории вероятностей, и теории случайных процессов и их использовании при решении научных и прикладных задач, выработка у студентов умения проводить статистический анализ прикладных и овладение основными методами исследования и решения таких задач, выработка у студентов умения проводить статистический анализ прикладных и овладение основными методами исследования и решения таких задач. 2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Теория вероятностей, математическая статистика входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения),</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i> 108 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>сформированные в результате изучения дисциплин/ практик: Математический анализ Информатика Теория информации Алгебра и геометрия Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Дискретная математика Исследование операций и теория игр Основы теории оптимизации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Теория вероятностей, математическая статистика» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 - Способностью 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</p> <p>Знать Основные методы исследований, используемых в теории вероятностей и математической статистике Основные законы, правила и определения процессов</p> <p>Уметь Выделять главное, существенное при решении поставленных задач Обсуждать способы эффективного решения поставленных задач Распознавать эффективное решение от неэффективного Объяснять (выявлять и строить) типичные модели поставленных задач</p> <p>Владеть Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат теории вероятностей, математической статистики, в том числе с использованием вычислительной техники.</p> <p>Дисциплина включает в себя следующие разделы: 1. Теория вероятностей 1.1. Элементы теории множеств, комбинаторики и теории меры. Аксиоматика теории вероятностей. Независимость событий и условные вероятности. Классические вероятностные схемы и классические предельные теоремы. Случайные величины и случайные векторы. Числовые характеристики случайных величин.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.2.Характеристические функции Вероятностный метод в приложении к задачам комбинаторики и теории двоичных функций.</p> <p>2. Математическая статистика</p> <p>2.1. Основные понятия математической статистики. Точечное оценивание параметров распределения. Интервальное оценивание параметров распределения. Проверка статистических гипотез (параметрическая статистика). Проверка статистических гипотез (непараметрическая статистика).</p> <p>2.2. Последовательный статистический анализ. Метод статистических испытаний.</p>	
Б1.Б.14	<p>Дискретная математика</p> <p>1 Цели освоения дисциплины (модуля) Целью дисциплины «Дискретная математика» является усвоение обучающимися базовых понятий дискретной математики, использование их для решения прикладных задач, а также формирование общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Дискретная математика входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Алгебра и геометрия Математический анализ Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Теория графов и ее приложения Математическая логика и теория алгоритмов Исследование операций и теория игр</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Дискретная математика» обучающийся должен обладать следующими компетенциями: ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации, в том числе с использованием вычислительной техники</p> <p>Знать Основные идеи комбинаторики, понятия теории множеств, булевой алгебры, теории конечных автоматов и графов</p> <p>Уметь Применять методы дискретной математики для решения практических задач Выбирать и применять методы дискретной математики и средства вычислительной техники для решения практических задач</p> <p>Владеть Навыками применения математического аппарата дискретной математики для формализации, анализа и выработки решения профессиональных задач с использованием вычислительной техники</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Комбинаторика</p> <p>1.1 Понятие выборки. Выборки упорядоченные и неупорядоченные. Размещения, сочетания, перестановки.</p> <p>1.2 Формула бинома Ньютона и следствие из нее.</p> <p>1.3 Алгоритм «Сочетания», алгоритм «Сочетания добавлением/изъятием одного элемента».</p> <p>1.4 Алгоритмы порождения перестановок: «Индуктивный» и «Транспозиция».</p> <p>2. Линейные и циклические коды</p> <p>2.1 Понятие линейного кода. Теорема о числе слов линейного кода. Порождающая и проверочная матрицы линейного кода и их связь</p> <p>2.2 Кодирование линейным кодом. Понятие циклического кода.</p> <p>2.3 Порождающая и проверочная матрицы циклического кода.</p> <p>3. Теория графов</p> <p>3.1 Основные понятия теории графов</p> <p>3.2 Эйлеровы и гамильтоновы графы</p> <p>3.3 Деревья</p> <p>3.4 Метрические характеристики графа</p> <p>4. Теория конечных автоматов</p> <p>4.1 Основные понятия теории автоматов</p> <p>4.2 Эквивалентность в автоматах. Эксперименты с автоматами</p>	
Б1.Б.15	<p>Математическая логика и теория алгоритмов</p> <p>1 Цели освоения дисциплины (модуля): Цель дисциплины - является усвоение студентами базовых понятий теории математической логики и теории алгоритмов, использование их для решения прикладных задач, создание основы для изучения других математических и естественнонаучных дисциплин, обеспечение теоретической и практической базы</p>	<p><i>Общая трудоемкость дисциплины составляет 4</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>подготовки специалистов к деятельности, связанной с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере. Задачи дисциплины - выработка умений и навыков использования теоретического материала при решении практических задач, создание научной и прикладной базы для последующего изучения математических и специальных дисциплин, а также формирование профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины(модуля) в структуре образовательной программы</p> <p>Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин:</p> <p>«Алгебра и геометрия», «Математический анализ», «Дискретная математика», «Информатика», «Теория информации», «Языки программирования».</p> <p>Знания(умения, владения),полученные при изучении данной дисциплины будут необходимы для изучения дисциплин /практик: Исследование операций и теория игр Теория графов и ее приложения Основы теории оптимизации Криптографические методы защиты информации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины(модуля)и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля)«Математическая логика и теория алгоритмов» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 способностью 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</p> <p>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</p>	<p>зачетных единицы 144 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>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. проводить верификацию программного обеспечения</p> <p>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</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Пропозициональная логика 1.1 Понятие пропозициональной переменной. Пропозициональные формулы. Пропозициональные связки. Система аксиом и теория формального вывода. Свойства формализованного исчисления высказываний. 1.2 Логическая равносильность формул. Нормальные формы. Алгоритмы построения нормальных конъюнктивных и дизъюнктивных форм. 1.3 Нормальные формы. Автоматизация полиномиального разложения. Метод неопределенных коэффициентов. Метод эквивалентных преобразований. Алгоритмы построения полиномиальной нормальной формы. 1.4 Применение булевых функций для построения релейно-контактных схем. Проектирование контроллеров на базе управляющих элементов булевых функций.</p> <p>2. Булевы функции 2.1 Булевы функции n аргументов. Минимизация булевых функций. Графический метод. 2.2 Алгоритмы минимизации булевых функций методом Карт Карно. Метод гиперкубов. 2.3 Полные системы функций. Базис булевых функций. Теорема Поста о функциональной полноте.</p> <p>3. Логика предикатов 3.1 Основные понятия, связанные с предикатами. Равносильность следованию предикатов. Логические икванторные операции над предикатами. 3.2 Использование метода резолюций для предикативного вывода. Проблемы разрешения для общезначимости и выполнимости</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>формул.</p> <p>4. Элементы теории алгоритмов</p> <p>4.1 Модели вычислений. Вычислительные парадигмы и задачи</p> <p>5. Конечные автоматы</p> <p>5.1 Нормальные алгорифмы Маркова. Алфавит, слова, конкатенация слов, подслова и вхождения. Расширение алфавита и алгорифмы над алфавитом. Нормально вычислимые функции</p> <p>5.2 Машины Тьюринга. ДМТ. НДМТ.</p> <p>5.3 Машины Поста. Эквивалентность моделей и тезис Чёрча—Тьюринга.</p> <p>6. Теория вычислимости</p> <p>6.1 Примитивная рекурсивность. Рекурсивные и примитивно рекурсивные отношения. Ограниченная квантификация и ограниченный поиск. Алгоритмы и разрешимость. Неразрешимые алгоритмические проблемы</p> <p>7. Основы логического программирования</p> <p>7.1 Основные конструкции языка программирования Пролог. Рекурсивное программирование.</p> <p>7.2 Метод отсечения и отката. Метод повтора. Списки и их использование. Вычислительная модель логических программ</p> <p>8. Алгоритмы параллельного программирования</p> <p>8.1 Этапы проектирования алгоритмов в парадигме параллельного программирования. Виды параллелизма. Максимальный теоретический выигрыш. Закон Амдала. Максимально допустимое ускорение Закон Густафсона-Барсиса.</p> <p>9. Алгоритмы генетического программирования</p> <p>9.1 Концепция построения генетического алгоритма. Генетические операторы. Концептуальные вопросы сферы применения, преимуществ и недостатков ГА.</p> <p>10. Верификация программ</p> <p>10.1 Правильные программы. Императивные программы. Задача верификации программ. Логика Хоара. Автоматическая проверка правильности программ</p> <p>10.2 Верификация распределенных программ. Логика линейного времени PLTL. Размеченные системы переходов. Задача верификации моделей программ.</p>	
Б1.Б.16	<p>Теория информации</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями дисциплины «Теория информации» является приобретение обучающимися основных понятий о природе информации, как объективной сущности, в парадигме Шеннона. Подробно описаны основные подходы к оценке количества информации. В хронологическом порядке даны основные способы кодирования информации как эффективного, так и помехоустойчивого.</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетн</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Овладение обучающимися необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Теория информации входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Информатика Алгебра и геометрия Организация ЭВМ и вычислительных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Безопасность сетей ЭВМ Физические основы передачи информации Техническая защита информации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Теория информации» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> - основы теории информации; - способы измерения количественных характеристик информации; - способы измерения качественных характеристик информационных систем; - основные методы эффективного кодирования; - основные методы помехозащищенного кодирования; <p>Уметь</p> <ul style="list-style-type: none"> - 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; 	<p><i>ых единицы</i> 180 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <ul style="list-style-type: none"> - профессиональным языком предметной области знания; - современными методиками кодирования; - методиками оценки эффективности алгоритмов сжатия; - методиками оценки эффективности алгоритмов помехоустойчивого кодирования; <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Основы теории информации <ol style="list-style-type: none"> 1.1 Возникновение теории информации. Системы передачи информации. Основные понятия. Задачи и постулаты прикладной теории информации. 1.2 Количественная оценка информации. Энтропия. Свойства энтропии. Энтропия при непрерывном сообщении. Условная энтропия. Взаимная энтропия. Избыточность информации. Коэффициенты сжатия и избыточности. 2. Методы кодирования, основанные на статистических параметрах. <ol style="list-style-type: none"> 2.1 Методы архивации. Кодирование символами переменной длины (алгоритм Хаффмана). Кодирование изображения, звука и видео (метод Лемпеля - Зива). Эффективное кодирование. Двоично-десятичные коды. Метод Шеннона-Фано. Метод Хаффмана. 3. Помехоустойчивые коды <ol style="list-style-type: none"> 3.1 Кодирование информации для канала с помехами. Разновидность помехоустойчивых кодов. Общие причины использования избыточности. Разрешенные и запрещенные кодовые комбинации. Кодовое расстояние. Матрица 3.2 Исправление одиночных ошибок. Контроль по нечетности (четности). Линейные коды. Основные определения. Построение двоичного группового кода. 3.3 Коды Хемминга. Обнаружение одиночных ошибок. Исправление одиночных или обнаружение двойных ошибок. Обнаружение ошибок 4. Циклические коды. <ol style="list-style-type: none"> 4.1 Определение проверочных равенств. Максимальное декодирование групповых кодов. Матричное представление линейных кодов. Технические средства кодирования и декодирования 4.2 Построение циклических кодов. Порождающий многочлен. Методы образования циклического кода. Технические средства кодирования и декодирования 	
Б1.Б.17	<p>Информатика</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Информатика» является повышение исходного уровня владения информационными технологиями,</p>	<p><i>Общая трудоемкость дисциплины</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем общепрофессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>Специальная цель дисциплины: формирование представлений об основных принципах информатики, сферах ее применения, перспективах развития, способах функционирования и использования информационных технологий решения задач.</p> <p>Приоритетными объектами изучения информатики являются информационные системы, связанные с информационными процессами, и информационные технологии, рассматриваемые с позиций системного подхода.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Информатика входит в базовую часть учебного плана образовательной программы.</p> <p>Для освоения дисциплины обучающиеся используют знания, умения и компетенции, сформированные в ходе изучения базового курса «Информатика» в объеме средней общеобразовательной школы.</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Языки программирования Информационные технологии. Базы данных Теория информации Сети и системы передачи информации Технологии и методы программирования Основы теории оптимизации Основы информационной безопасности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Информатика» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> — Классификацию современных компьютерных систем; — Классификацию системного и прикладного программного 	<p><i>ины</i> <i>составл</i> <i>яет 12</i> <i>зачетны</i> <i>х</i> <i>единицы</i> 432 <i>акад.</i> <i>часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обеспечения;</p> <ul style="list-style-type: none"> — Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера. <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные понятия информатики; — Основные способы хранения, обработки и передачи информации; — Основы технологии поиска в современных информационно-поисковых системах; — Значение информации в развитии современного общества. <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>Дисциплина включает в себя следующие разделы:</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1. Основные понятия и сущность информационных ресурсов. Роль и значение информационных ресурсов в развитии информационных технологий и в информатизации общества</p> <p>1.1 Сущность и значение информации в развитии современного общества. Общая характеристика процесса сбора, передачи, обработки и накопления информации. Мировые информационные ресурсы. Виды информационных ресурсов. Способы хранения информации</p> <p>2. Операционные системы. Системное и прикладное программное обеспечение. Современные компьютерные системы.</p> <p>2.1 Системное и прикладное программное обеспечение. Обзор существующих операционных систем, их достоинства и недостатки. Операционная система как виртуальная машина. Операционная система как менеджер ресурсов. ОС WINDOWS, основные концепции.</p> <p>2.2 Программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска).</p> <p>2.3 Классификация современных компьютерных систем. Слои программного обеспечения компьютерной системы. Классификация прикладного программного обеспечения. Основные утилиты.</p> <p>3. Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.</p> <p>3.1 Технические средства реализации информационных процессов. Структура вычислительной системы. Основные характеристики современных компьютеров. Периферийное оборудование.</p> <p>4. Обеспечение безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).</p> <p>4.1 Основы защиты информации. Антивирус как средство защиты информации. Классификация вирусов, основные различия, проявления. Антивирусные программы.</p> <p>4.2 Архивация данных. Восстановление данных</p> <p>5. Типовые структуры и принципы организации компьютерных сетей</p> <p>5.1 Локальные и глобальные сети ЭВМ. Понятие локальных и глобальных сетей. Общие понятия и принципы функционирования сетей. Модель компьютерной связи. Глобальная сеть Интернет. Службы Интернета и их назначение. Защита информации в сети.</p> <p>6. Работа с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов)</p> <p>6.1 Средства представления и приемы обработки текстовой информации. Текстовый процессор Word. Основные приемы</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обработки текстовой информации. Этапы создания документа, редактирование, форматирование, печать текста. Вставка OLE-объектов (формулы, рисунки, WordArt). Работа с таблицами. Работа с элементами текста (разбивка на колонки, создание списков, автоматического оглавления, алфавитного указателя, гиперссылок). Создание шаблонов документов.</p> <p>6.2 Средства представления и приемы обработки презентационных материалов. Этапы и правила создания презентации, редактирование, форматирование, вставка графики и анимации, использование специальных эффектов.</p> <p>6.3 Средства представления и алгоритмы обработки числовой информации. Табличный процессор EXCEL. Назначение, основные приемы работы. Абсолютная и относительная адресация. Форматирование ячеек. Основные приемы построения формул. Стандартные функции. Отображение табличной информации в графической форме. Построение диаграмм. Сортировки, фильтры.</p> <p>6.4 Использование электронных таблиц при решении математических задач. Применение электронных таблиц в профессиональной деятельности. Модели решения функциональных и вычислительных задач. Модели решения задач с принятием решения по условию. Алгоритмы поиска по критерию. Решение задач оптимизации с помощью надстройки «Поиск решения».</p> <p>7. Использование языков, систем и инструментальных средств программирования в профессиональной деятельности. Алгоритмизация и программирование. Языки программирования высокого уровня.</p> <p>7.1 Автоматизация работы в EXCEL. Макропрограммирование в MS EXCEL, основные понятия, способы написания.</p> <p>7.2 Объектно-ориентированный язык программирования VBA. Основные элементы языка VBA, типы данных и переменные, применение операторов присваивания и встроенных функций. Ввод и вывод информации. Структура оператора принятия решений IF. Использование циклических алгоритмов (счетчики, операторы циклов с условием, циклы объектного типа). Вложенные структуры.</p> <p>7.3 Алгоритмы решения вычислительных задач. Работа с массивами данных. Поиск экстремума. Алгоритмы сортировки. Создание, применение процедур и функций Основные понятия объектно-ориентированного программирования, его применение в VBA. Основные объекты.</p> <p>7.4 Организация человеко-машинного интерфейса. Работа с формами и элементами управления. Программирование обработчиков событий.</p> <p>8. Применение достижений современных информационных</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации.</p> <p>8.1 Информационные системы. Структура и классификация ИС, специализированные ИС. Информационные системы, используемые в предметной области. Основные модели данных. СУБД, общее понятие, классификация.</p> <p>8.2 Базы данных. СУБД MS ACCESS. Проектирование баз данных. Создание запросов к БД (запросы на выборку, параметрические, запросы с групповыми операциями, перекрестные, запросы с вычисляемыми полями). Создание экранных форм, отчетов.</p> <p>9. Использование библиотек прикладных программ для решения прикладных математических задач.</p> <p>9.1 Программное обеспечение и технологии моделирования функциональных задач. Система компьютерной математики MathCAD. Представление информации в текстовых, графических, вычислительных блоках. Работа с формулами и функциями. Графическое представление данных. Операции с матрицами. Символьные вычисления в MathCAD.</p> <p>9.2 Модели решения функциональных задач. Классификация моделей и решаемых на их базе задач. Решение нелинейных уравнений, систем линейных и нелинейных уравнений. Решение дифференциальных уравнений (ОДУ первого и высших порядков). Решение задач оптимизации. Программирование в MathCAD.</p>	
Б1.Б.18	<p>Исследование операций и теория игр</p> <p>1 Цели освоения дисциплины (модуля) Целью курса является ознакомление студентов с основными принципам построения, применения и анализа математических моделей и их использования при разработке конкретных проектов.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Исследование операций и теория игр входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Алгебра и геометрия Математический анализ Дискретная математика Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Основы теории оптимизации Математическое моделирование распределенных систем</p> <p>3 Компетенции обучающегося, формируемые в результате</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Исследование операций и теория игр» обучающийся должен обладать следующими компетенциями: ОПК-2 Способностью 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 методы исследования операций и теории игр Определения основных понятий, называет их структурные характеристики Основные законы, правила и определения процессов Уметь Выделять главное, существенное при решении поставленных задач Обсуждать способы 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 Дисциплина включает в себя следующие разделы: 1. Основные понятия и методологические основы исследования операций 1.1. Введение в исследование операций. Основные понятия и методологические основы исследования операций 1.2.Методика определения полезности. Принятие решений в различных условиях. 2.Задачи массового обслуживания в исследовании операций 2.1. Введение в теорию массового обслуживания. Задачи массового обслуживания в рамках исследования операций 3. Элементы теории игр 3.1. Введение в теорию игр. Матричные игры. Решение матричных игр в чистых стратегиях. Принцип минимакса и максимина. Доминирующие стратегии. 3.2. Решение матричных игр в смешанных стратегиях 3.3. Игры с природой. Принятие решений в условиях неопределенности. Принятие решений в условиях риска</p>	
Б1.Б.19	Теория графов и ее приложения	<i>Общая</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1 Цели освоения дисциплины (модуля) Целями освоения дисциплины «Теория графов и ее приложения» являются: знакомство с фундаментальными понятиями и математическим аппаратом теории графов; изучение основных задач теории графов и методов их решения, формирование навыков эффективно применять алгоритмы обработки машинного представления графов для решения прикладных задач.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Теория графов и ее приложения входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Дискретная математика Математический анализ Языки программирования Теория информации Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Разработка и эксплуатация защищенных автоматизированных систем Криптографические методы защиты информации Методы выявления нарушений информационной безопасности, аттестация АИС Алгоритмы шифрования информации Моделирование угроз информационной безопасности Моделирование систем и процессов защиты информации Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика Научно-исследовательская работа</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Теория графов и ее приложения» обучающийся должен обладать следующими компетенциями: Структурный элемент компетенции Планируемые результаты обучения ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p>	<p><i>трудоёмкость дисциплины составляет 3 зачетных единиц</i> 108 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать</p> <ul style="list-style-type: none"> -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 <p>Уметь</p> <ul style="list-style-type: none"> -Использовать технологии автоматизированного проектирования информационных систем -Применять методы теории графов для построения модели нарушителя в автоматизированных системах <p>Владеть</p> <ul style="list-style-type: none"> -Навыками применения графовых алгоритмов для определения ресурсов, необходимых для обеспечения безопасности информационной системы -Методами построения моделей для контроля эффективности мер защиты информации <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> -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 <p>Уметь</p> <ul style="list-style-type: none"> -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 <p>Владеть</p> <ul style="list-style-type: none"> -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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-Навыками решения оптимизационных задач теории графов и задач сетевого планирования</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Машинное представление графов <ol style="list-style-type: none"> 1.1 Способы машинного представления графов. Структуры языков программирования высокого уровня для хранения и обработки информации в представлении графовых структур. Виды графов, подграфы, операции над графами. 2. Обходы графов <ol style="list-style-type: none"> 2.1 Связность, компоненты связности. Маршруты, цепи, пути, циклы. 2.2 Обходы графов: виды обходов, реализация обходов. 3. Каркасы и фундаментальные множества <ol style="list-style-type: none"> 3.1 Каркасы графа. Матрица Кирхгофа. Способы построения каркасов. Алгоритмы поиска каркаса минимального веса 3.2 Цикломатическое число графа. Фундаментальное множество (базис) циклов графа. 4. Компоненты сильной связности <ol style="list-style-type: none"> 4.1 Теорема Менгера. k- связность графа. Алгоритм нахождения компонент сильной связности графа. Применение алгоритма поиска компонент двусвязности для определения надежности сетей связи. 5. Разрезания и раскраска графов <ol style="list-style-type: none"> 5.1 Понятие разреза. Задача о разрезании графа. Разрезание различных видов графов. Понятие раскраски, хроматического числа. 5.2 Задача о вершинной раскраске, о раскраске граней, их связь. Оценка хроматического числа для некоторых видов графов. 6. Оптимизационные задачи на графах <ol style="list-style-type: none"> 6.1 Поиск кратчайших путей. Алгоритмы Форда-Беллмана, Флойда, Дейкстры, поиск пути в бесконтурном графе. 6.2 Задача коммивояжера. 6.3 Сетевое планирование. Задача о максимальном потоке. 7. Прикладные задачи теории графов <ol style="list-style-type: none"> 7.1 Применение графов для задач программирования, графы как модели программ, процессов, информационных структур. 7.2 Построение модели внутреннего нарушителя с применением теории графов. 7.3 Применении теории графов к моделированию СЗИ и управлению рисками информационной безопасности 8. Укладка графов <ol style="list-style-type: none"> 8.1 Задачи визуализации графов. Задачи плоской укладки графа. Теорема Понтрягина-Куратовского 	
Б1.Б.20	<p>Языки программирования</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Языки программирования» является изучение</p>	Общая трудоемкость

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>языков программирования высокого уровня и формирования у обучающихся навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Языки программирования» рассматривает основные подходы к проектированию программных средств, освоению методологий структурного и объектно-ориентированного программирования, а также методов тестирования и отладки программ.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Языки программирования входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Информатика Организация ЭВМ и вычислительных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Технологии и методы программирования Разработка и эксплуатация защищенных автоматизированных систем Основы теории оптимизации Математическое моделирование распределенных систем Криптографические методы защиты информации Алгоритмы шифрования информации Тестирование систем защиты информации автоматизированных систем Моделирование угроз информационной безопасности Моделирование систем и процессов защиты информации Защита программного обеспечения Методы проектирования защищенных распределенных информационных систем</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Языки программирования» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать Общие принципы построения современных языков программирования высокого уровня.</p>	<p><i>дисциплины составляет 9 зачетных единиц 324 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Общие принципы использования современных языков программирования высокого уровня.</p> <p>Язык программирования высокого уровня (объектно-ориентированное программирование).</p> <p>Уметь</p> <p>Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования.</p> <p>Проводить комплексное тестирование и отладку программных систем.</p> <p>Работать с интегрированной средой разработки программного обеспечения.</p> <p>Использовать шаблоны классов и средства макрообработки.</p> <p>Использовать динамически подключаемые библиотеки.</p> <p>Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.</p> <p>Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования.</p> <p>Владеть</p> <p>Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования.</p> <p>Навыками работы с интегрированной средой разработки программного обеспечения.</p> <p>Навыками проектирования программного обеспечения с использованием средств автоматизации.</p> <p>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</p> <p>Знать</p> <p>Способы разработки сложного программного обеспечения.</p> <p>Эффективные способы реализации структур данных и конкретных алгоритмов при решении различных задач.</p> <p>Требования, предъявляемые к разработке внешних спецификаций, для разрабатываемого программного обеспечения.</p> <p>Уметь</p> <p>Планировать разработку сложного программного обеспечения.</p> <p>Проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении различных задач.</p> <p>Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения.</p> <p>Владеть</p> <p>Навыками разработки типового программного обеспечения.</p> <p>Навыками разработки внешней спецификации для</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>разрабатываемого программного обеспечения. Навыками разработки сложного программного обеспечения. Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Методики разработки программ <ol style="list-style-type: none"> 1.1 Структурное программирование. Модульное программирование. Объектно-ориентированное программирование. 1.2 Стандарты построения блок-схем. Представление типовых алгоритмов в виде блок-схем. Среда программирования. 2. Языки программирования <ol style="list-style-type: none"> 2.1 Классификация языков программирования 2.2 Платформа .NET. Концепция языка программирования C# 2.3 Среда быстрой разработки приложений Visual Studio 3. Основы языка программирования C# <ol style="list-style-type: none"> 3.1 Структура программы C#. Типы данных. Создание консольных приложений 3.2 Функции и процедуры. Математические вычисления 3.3 Условный оператор. Оператор выбора. 3.4 Операторы цикла 3.5 Массивы и строки. Создание форм. Элементы управления форм для работы с массивами 4. Организация взаимодействия приложения с пользователем <ol style="list-style-type: none"> 4.1 Перехват и обработка ошибок. Обработка особых ситуаций 4.2 Обработка диалога с пользователем 5. Технологии работы в C# <ol style="list-style-type: none"> 5.1 Способы работы с файлами. Создание файловых переменных. Извлечение данных из файлов. Сохранение данных в текстовый файл 5.2 Классы: Основные понятия. Иерархии классов 5.3 Интерфейсы и структурные типы 5.4 Динамическое распределение памяти. Динамические структуры данных 5.5 Сборки, библиотеки, директивы 5.6 Программирование под Windows. Введение в графику 6. Создание пользовательских приложений <ol style="list-style-type: none"> 6.1 Технологии создания пользовательских приложений под Windows 	
Б1.Б.21	<p>Технологии и методы программирования 1 Цели освоения дисциплины (модуля) Целью дисциплины «Технологии и методы программирования» является изучение основ современных методов и средств программирования и формировании у обучающихся навыков их практического применения в соответствии с требованиями ФГОС ВО для специальности «Информационная безопасность автоматизированных систем». Дисциплина «Технологии и методы</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетны</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>программирования» рассматривает основные подходы к проектированию программных средств, освоении методологий структурного и объектно-ориентированного программирования, а также методов тестирования и отладки программ.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Технологии и методы программирования входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Организация ЭВМ и вычислительных систем Информатика Языки программирования Информационные технологии. Базы данных Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Криптографические методы защиты информации Тестирование систем защиты информации автоматизированных систем Моделирование угроз информационной безопасности Защита электронного документооборота Управление информационной безопасностью Анализ безопасности программного обеспечения Моделирование систем и процессов защиты информации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Технологии и методы программирования» обучающийся должен обладать следующими компетенциями:</p> <p>Структурный элемент компетенции</p> <p>Планируемые результаты обучения</p> <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать</p> <p>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</p>	<p>х единицы 216 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>соответствии с современными технологиями и методами программирования;</p> <p>Принципы организации документирования разработки, процесса сопровождения программного обеспечения.</p> <p>Уметь</p> <p>Работать с интегрированной средой разработки программного обеспечения;</p> <p>Использовать динамически подключаемые библиотеки;</p> <p>Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;</p> <p>Использовать шаблоны классов и средства макрообработки;</p> <p>Проводить комплексное тестирование и отладку программных систем;</p> <p>Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;</p> <p>Проводить выбор эффективных способов реализации профессиональных задач;</p> <p>Планировать разработку сложного программного обеспечения;</p> <p>Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;</p> <p>автоматизированных систем;</p> <p>Владеть</p> <p>Основными навыками проектирования программного обеспечения с использованием средств автоматизации.</p> <p>Навыками программирования различными стилями.</p> <p>Навыками разработки программной документации.</p> <p>Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.</p> <p>Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.</p> <p>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</p> <p>Знать</p> <p>Современные технологии программирования.</p> <p>Области и особенности применения языков программирования высокого уровня;</p> <p>Основные виды интегрированных сред разработки программного обеспечения.</p> <p>Основные методы эффективного кодирования.</p> <p>Способы обработки исключительных ситуаций;</p> <p>Современные технологии и методы программирования,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>предназначенные для создания прикладных программ.</p> <p>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.</p> <p>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.</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Введение в технологии программирования <ol style="list-style-type: none"> 1.1 Языки и парадигмы программирования. Инструментальные средства для разработки программных средств. Компиляторы и интерпретаторы. Классификация технологических подходов. Коллективная разработка ПО. 1.2 Жизненный цикл программных средств. Модели жизненного цикла. Каскадная, инкрементная и спиральная модели. Понятие качества программного средства. 2. Проектирование и разработка архитектуры <ol style="list-style-type: none"> 2.1 Основные подходы к проектированию ПО. 2.2 Тестирование и отладка ПО. Документация и сопровождение ПО. 3. Преимущества языка Python <ol style="list-style-type: none"> 3.1 Особенности языка. Преимущества языка Python. 4. Язык программирования Python <ol style="list-style-type: none"> 4.1 Основы языка. Типы данных. 4.2 Операторы ветвления, циклы. Функции. 4.3 Структуры данных: списки (lists), кортежи (tuples) и словари (dictionaries). 4.4 Классы: Основные понятия. Иерархии классов. 4.5 Работа с файловой системой. 4.6 Библиотеки, импорт библиотек. 4.7 Обработка исключений. 4.8 Подготовка к зачету 5. Основы Web-программирования. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>5.1 Стандарт SGML.</p> <p>5.2 Структура документа. Модель DOM. Основы HTML. Основные тэги. Достоинства и недостатки.</p> <p>5.3 Основы XML. Структура документа XML и иерархия информации. Основные компоненты и тэги. Применение таблиц стилей CSS и рекомендаций XSL.</p> <p>6. Языки сценариев</p> <p>6.1 Клиент-серверное и межплатформенное программирование.</p> <p>6.2 Языки клиентских сценариев. Основы JavaScript. Особенности отладки и тестирования клиентских приложений.</p> <p>6.3 Модель DOM. Работа с массивами и коллекциями.</p> <p>6.4 Язык сценариев общего назначения PHP. Основы PHP: типы данных, операторы.</p> <p>6.5 Использование массивов. Создание функций.</p> <p>6.6 Подготовка курсовой работы</p> <p>6.7 Подготовка к экзамену</p>	
Б1.Б.22	<p>Электроника и схемотехника</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями изучения дисциплины являются: ознакомление студентов с законами преобразования и способами передачи информационных сигналов в электронных устройствах и линиях связи; формирование знаний в области схемотехники аналого-вых и цифровых электронных устройств</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Электроника и схемотехника входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Алгебра и геометрия</p> <p>Информатика</p> <p>Физика</p> <p>Математический анализ</p> <p>Дискретная математика</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Программно-аппаратные средства обеспечения информационной безопасности</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Электроника и</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>схемотехника» обучающийся должен обладать следующими компетенциями:</p> <p>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</p> <p>Знать основы теории электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры</p> <p>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</p> <p>Владеть навыками работы с программными средствами схемотехнического моделирования; навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы</p> <p>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать Математические методы расчёта электрических цепей, теорию четырёхполюсников, Фурье преобразование и преобразования Лапласа, основы цифровой обработки сигналов</p> <p>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</p> <p>Владеть Навыками проектирования схем аналоговой и цифровой электроники для обработки информации</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Электрические цепи, сигналы <ol style="list-style-type: none"> 1.1 Электрические цепи 1.2 Цепи при гармоническом воздействии 1.3 Методы анализа сложных электрических цепей 1.4 Четырёхполюсники, фильтры и длинные линии связи 1.5 Сигналы и их спектры 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	2. Схемотехника 2.1 Полупроводниковые приборы 2.2 Электронные усилители и преобразователи сигналов 2.3 Нелинейные преобразователи сигналов 2.4 Импульсные и цифровые устройства 2.5 Цифровая обработка сигналов	
Б1.Б.23	<p>Безопасность операционных систем</p> <p>1 Цели освоения дисциплины (модуля) Целями освоения дисциплины (модуля) «Безопасность операционных систем» являются:</p> <p>1. Знакомство студентов с назначением, разновидностями и основными принципами организации современных операционных систем в объеме, достаточном для понимания задач обеспечения безопасности операционных систем.</p> <p>2. Обучение студентов принципам построения защиты информации в операционных системах (ОС) и методам анализа надежности защиты ОС.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Безопасность операционных систем входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Информатика Безопасность сетей ЭВМ Сети и системы передачи информации Организация ЭВМ и вычислительных систем Основы информационной безопасности</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Разработка и эксплуатация защищенных автоматизированных систем Информационная безопасность распределенных информационных систем Управление информационной безопасностью Моделирование угроз информационной безопасности Программно-аппаратные средства обеспечения информационной безопасности Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Производственная-преддипломная практика</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p align="center">3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Безопасность операционных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>Знать</p> <ul style="list-style-type: none"> - правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем - критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей ОС; <p>Уметь</p> <ul style="list-style-type: none"> - реализовывать политику учетных записей пользователей операционной системы; - сформировать комплекс мер защиты информации ограниченного доступа для операционной системы; <p>Владеть</p> <ul style="list-style-type: none"> - навыками формальной постановки задачи обеспечения информационной безопасности операционной системы. - навыками эксплуатации операционных систем и программных систем с учетом требований по защите информации ограниченного доступа; - навыками использования программно-аппаратных средств обеспечения информационной безопасности <p>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p> <p>Знать</p> <ul style="list-style-type: none"> - иметь представление об основных средствах защиты ОС в составе информационно-технологических ресурсов автоматизированной системы; - критерии защищенности ОС и сети ЭВМ; - критерии оценки эффективности и надежности средств защиты операционных систем; - принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; <p>Уметь</p> <p>использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- проводить мониторинг угроз безопасности операционных систем - 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 встроенных средств защиты информации ОС; - навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети; 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; Уметь - разрабатывать политику учетных записей пользователей ОС; - обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ; Владеть - навыками использования операционных систем семейств Unix и Windows в системах защиты информации ; - методами и технологиями исследования безопасности операционных систем. ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах 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;</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Уметь</p> <ul style="list-style-type: none"> -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; <p>Владеть</p> <ul style="list-style-type: none"> - 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 <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Предмет безопасности операционных систем <ol style="list-style-type: none"> 1.1 Основные понятия и положения защиты информации в информационно-вычислительных системах 1.2 Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем 2. Операционная система с точки зрения специалиста по информационной безопасности <ol style="list-style-type: none"> 2.1 Общая концепция построения ОС, виды ОС. 2.2 ОС семейства Unix и Windows. Концепции в обеспечении защиты 3. Структурная схема ОС <ol style="list-style-type: none"> 3.1 Центральные элементы ОС – ядро, пользовательская оболочка, файловая подсистема, сетевая под-система 3.2 Периферийные подсистемы ОС. Загрузка ОС и ее этапы 4. Многозадачные ОС <ol style="list-style-type: none"> 4.1 Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС 4.2 Принципы организации межпрограммного взаимодействия 5. Сетевая подсистема ОС <ol style="list-style-type: none"> 5.1 Сетевые сервисы ОС 5.2 Принципы построения сетевой подсистемы ОС Характерные уязвимости сетевой подсистемы ОС 6. Подготовка к промежуточной аттестации(зачет) <ol style="list-style-type: none"> 6.1 Подготовка к промежуточной аттестации 7. Подсистема безопасности ОС <ol style="list-style-type: none"> 7.1 Подсистема безопасности ОС. Основные компоненты 7.2 Модели безопасности в различных семействах ОС 7.3 Дискреционный и мандатный принципы управления доступом – сравнительный анализ 8. Администрирование операционных систем 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>8.1 Модели пользователей в различных ОС</p> <p>8.2 Профиль пользователя, бюджет, авторизация, аутентификация пользователя ОС</p> <p>8.3 Назначение прав пользователю ОС и аудит его действий</p> <p>8.4 Аудит системных событий ОС</p> <p>9. Противодействие атакам на информационные системы</p> <p>9.1 Методология атаки и их разновидности</p> <p>9.2 Методы обнаружения и предотвращения атак на информационные системы</p> <p>10. Подготовка к итоговой аттестации</p> <p>10.1 Экзамен</p>	
Б1.Б.24	<p>Безопасность сетей ЭВМ</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Безопасность сетей ЭВМ» являются овладение студентами необходимым и достаточным уровнем общепрофессиональных, профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Специальными целями освоения дисциплины (модуля) «Безопасность сетей ЭВМ» являются:</p> <ol style="list-style-type: none"> 1. Обучение обучающихся организации защиты сетевых устройств и каналов передачи информации, обнаружения и предотвращения несанкционированного доступа к информации в сетях ЭВМ. 2. Обучение обучающихся принципам построения систем защиты информации в локальных вычислительных сетях (ЛВС) и методам анализа надежности защиты ЛВС <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Безопасность сетей ЭВМ входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Информатика</p> <p>Сети и системы передачи информации</p> <p>Основы информационной безопасности</p> <p>Организация ЭВМ и вычислительных систем</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>Информационная безопасность распределенных информационных систем</p> <p>Моделирование угроз информационной безопасности</p> <p>Управление информационной безопасностью</p>	<p><i>Общая трудоемкость дисциплины составляет 7 зачетных единиц</i></p> <p>252</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Методы проектирования защищенных распределенных информационных систем Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Производственная-преддипломная практика 3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Безопасность сетей ЭВМ» обучающийся должен обладать следующими компетенциями: ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа Знать - Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним; - Основные принципы методик противодействия перехвату и 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. ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий Знать — Нормативные и правовые акты в области защиты информации</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>передаваемой в сетях ЭВМ; — Современные технологии обеспечения информационной безопасности в сетях ЭВМ; — Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ.</p> <p>Уметь</p> <ul style="list-style-type: none"> - Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей; - Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности; - 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. <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Основные понятия безопасности сетей ЭВМ <ol style="list-style-type: none"> 1.1 Безопасность сетей ЭВМ – история вопроса, современное состояние, тенденции 1.2 Основные уязвимости сетей ЭВМ и их использование нарушителем 1.3 Парольная защита административного и консольного входов на сетевое оборудование 1.4 Защита удаленного подключения к сетевому оборудованию 2. Модель безопасности для локальной вычислительной сети <ol style="list-style-type: none"> 2.1 Принцип «обороны в глубину» как базовый принцип при организации защиты сети 2.2 Сегментирование ЛВС как способ повышения безопасности сети 2.3 Мониторинг состояния транспортной подсистемы как средство контроля за состоянием сетевой безопасности 3. Обнаружение и нейтрализация сетевых атак <ol style="list-style-type: none"> 3.1 Понятие «сетевой атаки» - история, классификация, современный подход к вопросу 3.2 Фазы сетевой атаки 3.3 Методики обнаружения сетевых атак 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>3.4 Основные меры противодействия сетевым атакам; системы обнаружения и предотвращения вторжений</p> <p>4. Технологии безопасности локальных вычислительных сетей</p> <p>4.1 Технология виртуальных ЛВС (VLAN)</p> <p>4.2 Технология Port Security</p> <p>4.3 Технология списков контроля доступа (ACL)</p> <p>5. Подготовка к промежуточной аттестации</p> <p>6. Методы контроля сетей ЭВМ</p> <p>6.1 Анализ сетевого трафика</p> <p>6.2 Перехват сетевых сообщений</p> <p>6.3 Использование защищенных протоколов для защиты сетевого трафика</p> <p>7. Безопасность беспроводных сетей</p> <p>7.1 Устройство и разновидности беспроводных сетей</p> <p>7.2 Проблема безопасности в беспроводных сетях</p> <p>8. Защищенные сети</p> <p>8.1 Понятие защищенной сети</p> <p>8.2 Технология виртуальной частной/защищенной сети (VPN). Классификация сетей VPN</p> <p>8.3 Разновидности технологий VPN</p> <p>8.4 Алгоритмы шифрования, применяемые для организации VPN</p> <p>9. Подготовка к итоговой аттестации и курсовой</p> <p>9.2 Подготовка к итоговой аттестации</p>	
Б1.Б.25	<p>Безопасность систем баз данных</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Безопасность систем баз данных» является изучение реализации политики безопасности баз данных и формирование у обучающихся навыков ее практического применения в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Безопасность систем баз данных» рассматривает основные принципы и основные направления обеспечения безопасности данных.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Безопасность систем баз данных входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Организация ЭВМ и вычислительных систем</p> <p>Введение в специальность</p> <p>Языки программирования</p> <p>Сети и системы передачи информации</p> <p>Основы информационной безопасности</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетных единиц</i></p> <p>216</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Информационные технологии. Базы данных</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Технология построения защищенных распределенных приложений</p> <p>Информационная безопасность распределенных информационных систем</p> <p>Тестирование систем защиты информации автоматизированных систем</p> <p>Защита электронного документооборота</p> <p>Методы мониторинга информационной безопасности АС</p> <p>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>Управление информационной безопасностью</p> <p>Информационная безопасность систем организационного управления</p> <p>Научно-исследовательская работа</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Безопасность систем баз данных» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>Знать</p> <p>Методы формирования требований по защите информации, обрабатываемой в СУБД.</p> <p>Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.</p> <p>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.</p> <p>Организационные меры по защите информации, обрабатываемой в СУБД.</p> <p>Уметь</p> <p>Использовать методы формирования требований по защите информации, обрабатываемой в СУБД.</p> <p>Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.</p> <p>Организовывать безопасность АРМ, на которых установлена СУБД.</p> <p>Владеть</p> <p>Методами формирования требований по защите информации,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обрабатываемой в СУБД. Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД. ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>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</p> <p>Уметь Настраивать систему организации и контроля доступа различного вида. Анализировать и находить решения по защите от атак на системы</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>данных, использующих различные виды аутентификации. Устанавливать средства защиты БД. Владеть</p> <p>Навыками настройки и администрирования средств защиты БД. Навыками разработки системы защиты с учетом особенностей защиты информации, обрабатываемой в СУБД. Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.</p> <p>Дисциплина включает в себя следующие разделы</p> <p>1. Общие положения обеспечения безопасности доступа к данным. 1.1 Предмет и содержание дисциплины. Обеспечение безопасности доступа к данным. 1.2 Задачи защиты информации обеспечения безопасности доступа к данным. 2. Обеспечение надежной аутентификации. 2.1 Факторы аутентификации. 2.2 Аутентификация с использованием OTP-токенов. Аутентификация с помощью биометрических характеристик. Анализ недостатков методов. 3. Управление доступом к данным. 3.1 СКУД на базе контактных смарт-карт. СКУД на базе бесконтактных RFID смарт-карт. СКУД на базе биометрических систем. 3.2 СКУД на базе ключей eToken. СКУД на базе ключей iButton. 4. Парольные политики. 4.1 Методы парольной аутентификации. 4.2 Аутентификация с помощью запоминаемого пароля. Недостатки методов аутентификации с помощью запоминаемого пароля. 6. Документирование баз данных с учетом требований по обеспечению информационной безопасности. 6.1 Классы безопасности. Требования, предъявляемые к различным классам безопасности. 6.2 Требования к документации с учетом класса безопасности. 7. Атаки на системы данных. 7.1 Атаки на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них. 7.2 Атаки на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них. 7.3 SQL-инъекции 8. Применение средств криптографической защиты информации (СКЗИ). 8.1 Применение средств криптографической защиты информации</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>(СКЗИ), хранящейся в базах данных, от НСД. 8.2 Способы и средства криптографической защиты баз данных. 9. СКЗИ «Крипто БД». 9.1 Состав и совместимость СКЗИ «Крипто БД». Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД». 9.2 Использование «Крипто БД» в облачных средах. Основные принципы работы «Крипто БД». 9.3 Анализ угроз и уязвимостей СУБД Oracle :</p>	
Б1.Б.26	<p>Основы информационной безопасности 1 Цели освоения дисциплины (модуля) Целью дисциплины «Основы информационной безопасности» является понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной безопасности Российской Федерации. Формирование у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации. 2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Основы информационной безопасности входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Физика Информатика Введение в специальность Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Организационное и правовое обеспечение информационной безопасности Информационная безопасность распределенных информационных систем Методы проектирования защищенных распределенных информационных систем 3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Основы информационной безопасности» обучающийся должен обладать</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i> 108 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>следующими компетенциями: ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</p> <p>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 сфере. 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.</p> <p>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.</p> <p>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. ПК-3 способностью проводить анализ защищенности автоматизированных систем</p> <p>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.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Технические средства контроля эффективности мер защиты информации.</p> <p>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.</p> <p>Уметь</p> <p>Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.</p> <p>Анализировать основные узлы и устройства современных автоматизированных систем.</p> <p>Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах.</p> <p>Эффективно использовать современные компьютерные технологии для изучения предмета исследования.</p> <p>Владеть</p> <p>Представлением о возможности использования информационных технологий для решения профессиональных задач.</p> <p>Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности.</p> <p>Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.</p> <p>Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.</p> <p>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <p>Основные информационные технологии, используемые в автоматизированных системах.</p> <p>Сущность и понятие информационной безопасности и характеристику ее составляющих.</p> <p>Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.</p> <p>Уметь</p> <p>Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.</p> <p>Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности.</p> <p>Анализировать современную научно-техническую информацию по информационной безопасности.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе</p> <p>Владеть</p> <p>Основными методами научного познания в области защиты информации.</p> <p>Навыками участия в проведении исследовательских работ по информационной безопасности.</p> <p>Профессиональной терминологией в области информационной безопасности.</p> <p>Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах</p> <p>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p>Знать</p> <p>Основные меры по защите информации в автоматизированных системах.</p> <p>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p>Принципы организации работы малых коллективов исполнителей.</p> <p>Уметь</p> <p>Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.</p> <p>Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p> <p>Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.</p> <p>Владеть</p> <p>Профессиональной терминологией в области информационной безопасности.</p> <p>Навыками участия в проведении исследовательских работ по информационной безопасности.</p> <p>Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Место и роль информационной безопасности в системе национальной безопасности</p> <p>1.1 Сущность и понятие информации. Понятие национальной безопасности. Основы государственной информационной политики</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.2 Угрозы национальной безопасности страны во всех сферах деятельности государства все осуществляемые через информационную среду</p> <p>2. Классификация защищаемой информации и угроз информационной</p> <p>2.1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности</p> <p>2.2 Источники и классификация угроз информационной безопасности для объектов информатизации</p> <p>3. Способы обеспечения информационной безопасности</p> <p>3.1 Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации</p> <p>3.2 Классификация средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации</p> <p>4. Методы формирования требований по защите информации</p> <p>4.1 Анализ существующих методов и средств, применяемых для защиты информации</p> <p>4.2 Разработка предложений по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению их эффективности</p>	
Б1.Б.27	<p>Криптографические методы защиты информации</p> <p>1 Цели освоения дисциплины (модуля) Целью дисциплины «Криптографические методы защиты информации» является ознакомление обучающихся с основным понятием криптографии; моделям шифров и математическим методам их исследования; требованиям, предъявляемым к шифрам и основным характеристикам шифров; основополагающими принципами защиты информации на основе криптографических методов; криптографическими стандартами и их использовании в информационных системах; с реализацией криптографических методов на практике; в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Криптографические методы защиты информации входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Введение в специальность Организация ЭВМ и вычислительных систем Теория информации</p>	<p><i>Общая трудоемкость дисциплины составляет 7 зачетных единиц</i> 252 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Информатика Языки программирования Теория вероятностей, математическая статистика Математический анализ Основы информационной безопасности Теория графов и ее приложения Математическая логика и теория алгоритмов Исследование операций и теория игр Технологии и методы программирования Программно-аппаратные средства обеспечения информационной безопасности Основы теории оптимизации Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Защита электронного документооборота Алгоритмы шифрования информации Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Управление информационной безопасностью Защита программного обеспечения Информационная безопасность систем организационного управления Методы проектирования защищенных распределенных информационных систем Моделирование систем и процессов защиты информации Научно-исследовательская работа</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Криптографические методы защиты информации» обучающийся должен обладать следующими компетенциями: ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации Знать</p> <ul style="list-style-type: none"> • 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, 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>подстановкой, гаммированием, использованием таблицы Виженера.</p> <ul style="list-style-type: none"> • 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. <p>Уметь</p> <ul style="list-style-type: none"> • 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. <p>Владеть</p> <ul style="list-style-type: none"> • 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. <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> • 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>симметричных блочных криптосистем</p> <p>Уметь</p> <ul style="list-style-type: none"> • 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 <p>Владеть</p> <ul style="list-style-type: none"> • навыками использованием вычислительной техники для реализации криптографических алгоритмов <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Введение в криптографию. Основные классы шифров и их свойства</p> <p>1.1 История криптографии. Основные понятия криптографии. Модели шифров. Основные этапы становления криптографии как науки. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Основные требования к шифрам.</p> <p>1.2 Шифры перестановки. Шифры замены. Поточные шифры. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок. Одноалфавитные и многоалфавитные замены.</p> <p>1.3 Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных.</p> <p>1.4 Надежность шифров. Имитостойкость шифров. Помехоустойчивость шифров. Криптографическая стойкость шифров. Имитация и подмена сообщения. Характеристика имитостойкости шифров. Коды аутентификации. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.</p> <p>2. Принципы построения криптографических алгоритмов</p> <p>Реализация криптографических алгоритмов</p> <p>2.1 Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Методы получения случайных и псевдослучайных последовательностей. Методы усложнения последовательностей псевдослучайных чисел. Методы криптоанализа. Понятие криптоатаки. Классификация криптоатак. Классификация методов анализа криптографических алгоритмов</p> <p>2.2 Шифры с открытыми ключами Криптосистемы RSA и Эль-</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Гамалы. Преимущества асимметричных систем шифрования. Криптографические хэш-функции. Характеристики и алгоритмы выработки хэш-функций.</p> <p>2.3 Модели криптографических протоколов Понятие криптографического протокола. Основные примеры, классификация криптографических протоколов. Понятие электронной цифровой подписи. Стандарты ЭЦП.</p> <p>2.4 Разграничение и контроль доступа пользователей к техническим средствам вычислительной сети АПМДЗ «КРИПТОН-ЗАМОК». Идентификация и аутентификация пользователей до запуска BIOS. Блокировка компьютера при НСД, накопление и ведение электронного журнала событий. Контроль целостности.</p> <p>2.5 Протоколы установления подлинности. Протоколы управления ключами. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы распределения ключей.</p>	
Б1.Б.28	<p>Организация ЭВМ и вычислительных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Организация ЭВМ и вычислительных систем» является формирование у обучающихся понятий об основных принципах организации технических средств ЭВМ и систем; о функциональной и структурной организации ЭВМ; о принципах построения основных устройств ЭВМ; о важнейших этапах и тенденциях в развитии цифровой, аналоговой и гибридной вычислительной техники; о методах оценки параметров ЭВМ и отдельных их устройств и овладение обучающимися необходимым и достаточным уровнем общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Организация ЭВМ и вычислительных систем входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Для изучения дисциплины необходимы знания , сформированные в результате изучения информатики, физики общеобразовательной школы (элементарные знания дискретной математики, систем исчисления, базовые представления об электромагнитном взаимодействии).</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i></p> <p>108</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Электроника и схемотехника Сети и системы передачи информации Техническая защита информации Безопасность сетей ЭВМ Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Организация ЭВМ и вычислительных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные элементы персонального компьютера и их функциональное назначение, базовые топологии автоматизированных систем; — 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. <p>Уметь</p> <ul style="list-style-type: none"> — Определять требуемый перечень компонентов ПК под конкретное техническое задание; — Определять основные неисправности ПК и подключенных к нему устройств; — Проектировать одноранговые вычислительные сети. <p>Владеть</p> <ul style="list-style-type: none"> — Навыками сборки ПК из отдельных комплектующих; — Навыками работы с осциллографом; — Навыками настройки адаптеров сетевых подключений <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать</p> <ul style="list-style-type: none"> — принципы построения и функционирования, примеры реализаций современных операционных систем; — принципы работы элементов и функциональных узлов 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>электронной аппаратуры; — типовые схемотехнические решения основных узлов и блоков электронной аппаратуры</p> <p>Уметь — применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); — работать с современной элементной базой электронной аппаратуры</p> <p>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</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. История развития вычислительной техники. 1.1 Этапы развития вычислительной техники. Концепция машины с хранимой памятью. Типы структур вычислительных машин и систем.</p> <p>2. Представление информации в вычислительных системах 2.1 Арифметические основы ЭВМ. Системы счисления. Непозиционные и позиционные системы счисления. Системы счисления, используемые в ЭВМ. Использование обратного и дополнительного двоичных кодов для реализации всех арифметических операций с помощью суммирующего устройства. 2.2 Цифровая и аналоговая формы представления информации. Представление информации электрическими сигналами.</p> <p>3. Архитектура и принципы работы основных логических блоков ЭВМ. 3.1 Основы построения ЭВМ. Внутренняя организация процессора. Аппаратная организация системы ввода-вывода информации компьютера. Выявление неисправности системы ввода-вывода информации компьютера</p> <p>4. Организация работы памяти ЭВМ. 4.1 Иерархическая структура памяти. Основная память ЭВМ. Оперативное и постоянное запоминающие устройства: назначение и основные характеристики. Виды адресации.</p> <p>5. Внутренние интерфейсы ЭВМ 5.1 Общая структура ПК с подсоединенными периферийными устройствами. Системная шина и ее параметры. Системная плата: архитектура и основные разъемы. Интерфейсные шины и связь с системной шиной. Внутренние интерфейсы ПК: шины ISA, EISA, VCF, VLB, PCI, AGP и их характеристики.</p> <p>5.2 Выявление неисправности ПК. Типовые программные средства</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>сервисного на-значения.</p> <p>6. Операционные системы ЭВМ.</p> <p>6.1 Архитектура современных ОС ЭВМ. Реестр ОС. Драйверы устройств и их роль в организации связи между ядром ОС и устройствами ПК.</p> <p>7. Информационные сети</p> <p>7.1 Локальные, корпоративные, глобальные информационные сети. Модели и структуры информационных систем. Базовые топологии. Сетевые программные и технические средства.</p>	
Б1.Б.29	<p>Техническая защита информации</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Техническая защита информации» является формирование профессиональных навыков обеспечения информационной защиты от съема информации по техническим каналам утечки информации, использования методов и средств инженерно-технической защиты информации и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Дисциплина «Техническая защита информации» рассматривает основные принципы и основные направления технической защиты информации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Техническая защита информации входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Организация ЭВМ и вычислительных систем</p> <p>Введение в специальность</p> <p>Физика</p> <p>Основы радиотехники</p> <p>Теория информации</p> <p>Основы информационной безопасности</p> <p>Электроника и схемотехника</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Управление информационной безопасностью</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>Информационная безопасность распределенных информационных систем</p> <p>3 Компетенции обучающегося, формируемые в результате освоения</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетных единиц</i></p> <p>216</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Техническая защита информации» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Знать</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации.</p> <p>Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.</p> <p>Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.</p> <p>Уметь</p> <p>Участвовать в настройке технических средств обеспечения информационной безопасности.</p> <p>Самостоятельно настраивать технические средства обеспечения информационной безопасности.</p> <p>Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации.</p> <p>Применять технические средства обеспечения информационной безопасности.</p> <p>Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.</p> <p>Владеть</p> <p>Техникой настройки технических средств обеспечения информационной безопасности.</p> <p>Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем.</p> <p>Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.</p> <p>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>Знать</p> <p>Классификацию технических средств перехвата информации</p> <p>Возможности технических средств перехвата информации</p> <p>Организацию защиты информации от утечки по техническим</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>каналам на объектах информатизации.</p> <p>Уметь</p> <p>Классифицировать технические средства перехвата информации.</p> <p>Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации</p> <p>Выявлять каналы утечки информации</p> <p>Проводить контроль эффективности мер по защите информации техническими средствами</p> <p>Владеть</p> <p>Средствами технической защиты информации.</p> <p>Методами технической защиты информации.</p> <p>Навыками проведения проверки защищенности информации и эффективности мер по защите информации</p> <p>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать</p> <p>Физические основы функционирования систем обработки и передачи информации.</p> <p>Основные физические явления и законы, используемые при построении средств защиты информации от утечки по техническим каналам.</p> <p>Технические каналы утечки информации.</p> <p>Уметь</p> <p>Применять соответствующий математический аппарат при проведении расчетов защищенности информации</p> <p>Контролировать безотказное функционирование технических средств защиты информации.</p> <p>Заменять отказавшие технические средства защиты информации.</p> <p>Владеть</p> <p>Навыками работы с нормативными правовыми актами в области технической защиты информации.</p> <p>Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Общие положения защиты информации техническими средствами</p> <p>1.1 Предмет и содержание дисциплины.</p> <p>Физические основы функционирования систем обработки и передачи информации</p> <p>1.2 Задачи защиты информации от утечки по техническим каналам.</p> <p>2. Технические каналы утечки информации</p> <p>2.1 Условия и особенности утечки информации. Структура канала утечки. Виды технических каналов утечки информации</p> <p>2.2 Условия образования каналов утечки. Характеристики каналов</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>утечки информации</p> <p>3. Акустический канал утечки информации</p> <p>3.1 Виды акустических каналов утечки информации. Способы перехвата и средства съема информации по акустическому каналу</p> <p>3.2 Способы и средства защиты от съема информации по акустическому каналу. Системы защиты от утечки информации по акустическому каналу</p> <p>4. Вибрационный канал утечки информации</p> <p>4.1 Виды вибрационных каналов утечки информации. Способы перехвата и средства съема информации по вибрационному каналу</p> <p>4.2 Способы и средства защиты от съема информации по вибрационному каналу. Системы защиты от утечки информации по вибрационному каналу.</p> <p>4.3 Подготовка к зачету</p> <p>5. Электромагнитный канал утечки информации</p> <p>5.1 Виды электромагнитных каналов утечки информации. Способы перехвата и средства съема информации по электромагнитному каналу.</p> <p>5.2 Способы и средства защиты от съема информации по электромагнитному каналу. Системы защиты от утечки информации по электромагнитному каналу</p> <p>6. Оптический канал утечки информации</p> <p>6.1 Виды оптических каналов утечки информации. Способы перехвата и средства съема информации по оптическому каналу</p> <p>6.2 Способы и средства защиты от съема информации по оптическому каналу. Системы защиты от утечки информации по оптическому каналу</p> <p>7. Радиоэлектронный канал утечки информации</p> <p>7.1 Диапазоны частот радиоэлектронного канала. Способы перехвата и средства съема информации по радиоэлектронному каналу</p> <p>7.2 Способы и средства защиты от съема информации по радиоэлектронному каналу. Системы защиты от утечки информации по радиоэлектронному каналу</p> <p>8. Поиск средств несанкционированного съема информации</p> <p>8.1 Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях.</p> <p>8.2 Контроль эффективности мер по защите информации техническими средствами</p>	
Б1.Б.30	<p>Сети и системы передачи информации</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Сети и системы передачи информации» являются овладение студентами необходимым и достаточным уровнем общепрофессиональных и</p>	<p><i>Общая трудоемкость дисциплины</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Специальными целями дисциплины «Сети и системы передачи информации» являются:</p> <p>1. Знакомство обучающихся с назначением, разновидностями и основными принципами организации и построения вычислительных сетей в объеме, достаточном для понимания задач обеспечения передачи информации по вычислительным сетям и телекоммуникационным каналам связи.</p> <p>2. Обучение обучающихся принципам передачи информации в вычислительных сетях и телекоммуникационных каналах связи.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Сети и системы передачи информации входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Информатика Основы информационной безопасности Организация ЭВМ и вычислительных систем Теория информации Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Безопасность сетей ЭВМ Разработка и эксплуатация защищенных автоматизированных систем Информационная безопасность распределенных информационных систем Управление информационной безопасностью Моделирование угроз информационной безопасности Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Сети и системы передачи информации» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования,</p>	<p><i>составляет 4 зачетных единицы</i> 144 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - Виды сетевых топологий; - Принципы передачи информации по телекоммуникационным каналам; - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - Классификацию сетевых протоколов. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - Методиками проектирования топологии вычислительных сетей; - Навыками определения и поиска неисправностей в сетях ЭВМ; - Навыками настройки сетевого оборудования. <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; - Принципы адресации в вычислительных сетях; - Принципы организации межсетевого взаимодействия и межсетевой передачи информации. <p>Уметь</p> <ul style="list-style-type: none"> - Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками. <p>Владеть</p> <ul style="list-style-type: none"> - Профессиональным языком и терминологией предметной области (сети ЭВМ); 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ).</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Основные понятия сетей ЭВМ <ol style="list-style-type: none"> 1.1 Сети ЭВМ – история, функциональное назначение, классификация 1.2 Принципы передачи информации по сетям ЭВМ 1.3 Классификация сетевого оборудования: назначение, принципы действия, основные базовые характеристики 1.4 Сетевые протоколы: назначение, разновидности, характеристики 2. Эталонная модель взаимодействия открытых систем <ol style="list-style-type: none"> 2.1 Эталонная модель (модель OSI) как фундаментальный принцип построения современных вычислительных сетей 2.2 Структурные уровни модели, принципы организации и функциональное назначение каждого из уровней 2.3 Стек протоколов TCP/IP как базовый стек протоколов современных сетей ЭВМ 3. Организация вычислительных сетей <ol style="list-style-type: none"> 3.1 Виды сетевых топологий 3.2 Классификация сетей – локальные, кампусные, глобальные сети. Сходства и различия 3.3 Принципы межсетевого взаимодействия 3.4 Организация вычислительных сетей на базе стека протоколов TCP/IP 4. Технологии передачи информации по телекоммуникационным каналам связи <ol style="list-style-type: none"> 4.1 Телекоммуникационные каналы связи – назначение и область применения 4.2 Принципы передачи информации по телекоммуникационным каналам 4.3 Применение телекоммуникационных каналов связи для организации межсетевого взаимодействия 5. Методы контроля сетей ЭВМ <ol style="list-style-type: none"> 5.1 Анализ сетевого трафика 5.2 Просмотр сетевых сообщений 6. Беспроводные сети <ol style="list-style-type: none"> 6.1 Устройство и разновидности беспроводных сетей 6.2 Создание защищенной беспроводной сети 7. Подготовка к промежуточной аттестации 	
Б1.Б.31	<p>Организационное и правовое обеспечение информационной безопасности</p> <p>1 Цели освоения дисциплины (модуля)</p>	<i>Общая трудоемкость</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Целями освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются: обучить обучающихся практическим навыкам работы с нормативно-правовой базой деятельности в области обеспечения безопасности информации. Знания и практические навыки, полученные в курсе «Организационное и правовое обеспечение информационной безопасности» используются обучаемыми при разработке курсовых и дипломных работ.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> • дать представление о законодательстве РФ в области информации; • ознакомить с системой защиты государственной тайны; • ознакомить с правилами лицензирования и сертификации в области защиты информации; • ознакомить с организационными методами защиты информации; • ознакомить с методами обеспечения информационной безопасности. <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Организационное и правовое обеспечение информационной безопасности входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Введение в специальность Основы информационной безопасности Информационная безопасность распределенных информационных систем</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Методы выявления нарушений информационной безопасности, аттестация АИС Моделирование угроз информационной безопасности Методы мониторинга информационной безопасности АС Защита электронного документооборота Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Разработка эксплуатационной документации на системы защиты информации автоматизированных систем Управление информационной безопасностью Анализ рисков информационной безопасности Защита программного обеспечения Информационная безопасность систем организационного управления Методы проектирования защищенных распределенных</p>	<p><i>дисциплины составляет 3 зачетных единицы 108 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационных систем Моделирование систем и процессов защиты информации Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» обучающийся должен обладать следующими компетенциями: ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>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;</p> <p>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</p> <p>Владеть -навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</p> <p>Знать -виды тайн, закрепленные в российском законодательстве -правовые основы организации защиты государственной тайны и конфиденциальной информации,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-задачи органов защиты государственной тайны и служб защиты информации на предприятиях</p> <p>-основы организационного и правового обеспечения информационной безопасности,</p> <p>-основные нормативные правовые акты в области обеспечения информационной безопасности</p> <p>- нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;</p> <p>-правовые основы организации защиты государственной тайны и конфиденциальной информации,</p> <p>-задачи органов защиты государственной тайны и служб защиты информации на предприятиях</p> <p>Уметь</p> <p>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности</p> <p>Владеть</p> <p>-навыками работы с нормативными правовыми актами</p> <p>-навыками подготовки деловой корреспонденции</p> <p>ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p> <p>Знать</p> <p>-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов</p> <p>Уметь</p> <p>-разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;</p> <p>применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности</p> <p>Владеть</p> <p>-способностью разрабатывать научно-техническую документацию</p> <p>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p> <p>Знать</p> <p>основные меры по защите информации в автоматизированных системах (организационные, правовые);</p> <p>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности</p> <p>Уметь</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия</p> <p>разрабатывать предложения по совершенствованию системы управления ИБ</p> <p>Владеть</p> <p>методами организации и управления деятельностью служб защиты информации на предприятии</p> <p>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> -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; <p>Уметь</p> <ul style="list-style-type: none"> -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 <p>Владеть</p> <ul style="list-style-type: none"> -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 предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Правовое обеспечение информационной безопасности <ol style="list-style-type: none"> 1.1 Законодательство РФ в области информационной безопасности: Основы законодательства Российской Федерации в области информационной безопасности. Понятие и виды защищаемой 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации. Основы международного законодательства в области защиты</p> <p>1.2 Правовой режим защиты государственной тайны: Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Система нормативных правовых актов, регламентирующая обеспечение сохранности сведений, составляющих государственную тайну в РФ.</p> <p>1.3 Лицензирование в области защиты информации: Понятие лицензирования. Нормативные правовые акты РФ, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации.</p> <p>1.4 Сертификация в области защиты информации: Понятие сертификации. Нормативные правовые акты РФ и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации.</p> <p>1.5 Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность.</p> <p>2. Организационное обеспечение информационной безопасности</p> <p>2.1 Понятие организационной защиты информации. Сущность организационных методов защиты информации.</p> <p>2.2 Анализ и оценка угроз информационной безопасности объекта. Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угроз.</p> <p>2.3 Оценка ущерба: Понятие ущерба. Методы и способы оценки ущерба.</p> <p>2.4 Служба безопасности объекта: Место службы безопасности объекта в общей структуре системы защиты государственной тайны и государственной системы защиты информации. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности.</p> <p>2.5 Средства и методы физической защиты объекта: Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового</p> <p>2.6 Организация и обеспечение режима секретности: Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
Б1.Б.32	<p>Программно-аппаратные средства обеспечения информационной безопасности</p> <p>1 Цели освоения дисциплины (модуля) Целью дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является формирование профессиональных навыков администрирования подсистем информационной безопасности автоматизированной системы и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных программно-аппаратных СЗИ в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» рассматривает базовые теоретические понятия, лежащие в основе программно-аппаратной защиты информации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Программно-аппаратные средства обеспечения информационной безопасности входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Организация ЭВМ и вычислительных систем Введение в специальность Теория информации Информатика Языки программирования Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Сети и системы передачи информации Основы информационной безопасности Информационные технологии. Базы данных Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Информационная безопасность распределенных информационных систем Криптографические методы защиты информации Методы выявления нарушений информационной безопасности, аттестация АИС Организационное и правовое обеспечение информационной безопасности Тестирование систем защиты информации автоматизированных систем Защита электронного документооборота</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i> 180 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Методы мониторинга информационной безопасности АС Моделирование угроз информационной безопасности Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Разработка эксплуатационной документации на системы защиты информации автоматизированных систем Управление информационной безопасностью Анализ безопасности программного обеспечения Защита программного обеспечения Информационная безопасность систем организационного управления Методы проектирования защищенных распределенных информационных систем Моделирование систем и процессов защиты информации Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Программно-аппаратные средства обеспечения информационной безопасности» обучающийся должен обладать следующими компетенциями: ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>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.</p> <p>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.</p> <p>Владеть Навыками работы с подсистемами системы информационной безопасности автоматизированной системы.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Навыками администрирования системы ИБ АС.</p> <p>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</p> <p>Знать</p> <p>Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ.</p> <p>Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.</p> <p>Уметь</p> <p>Исследовать эффективность контрольных проверок работоспособности применяемых программно-аппаратных средств защиты информации.</p> <p>Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей ИБ АС.</p> <p>Владеть</p> <p>Навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации.</p> <p>Навыками использования программно-аппаратных средств обеспечения ИБ АС.</p> <p>Навыками анализа программных, архитектурно-технических и схемотехнических решений компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.</p> <p>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Знать</p> <p>Виды программных и программно-аппаратных средств защиты информации.</p> <p>Принципы администрирования системы ИБ АС.</p> <p>Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.</p> <p>Уметь</p> <p>Самостоятельно настраивать программные и программно-аппаратные средства обеспечения ИБ.</p> <p>Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ.</p> <p>Применять программные и программно-аппаратные средства обеспечения ИБ.</p> <p>Владеть</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Техникой настройки программных и программно-аппаратных средств обеспечения ИБ. Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС. Навыками анализа архитектурно-технических и схмотехнических решений компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Общие положения защиты информации программно-аппаратными средствами.</p> <p>1.1 Предмет и содержание дисциплины. Принципы работы систем обработки и передачи информации.</p> <p>1.2 Задачи и методы защиты информации программно-аппаратными средствами.</p> <p>2. Задачи и методы защиты информации от НСД.</p> <p>2.1 Применение СЗИ от НСД для организации защищенных компьютерных систем.</p> <p>2.2 Электронные ключи и идентификаторы.</p> <p>3. СЗИ от НСД «СТРАЖ NT».</p> <p>3.1 Механизмы системы защиты СЗИ «СТРАЖ NT».</p> <p>Администрирование СЗИ. Аварийное снятие и восстановление системы защиты.</p> <p>3.2 Редактирование параметров системного аудита. Установка параметров целостности. Назначение грифа. Контроль устройств.</p> <p>4. Обеспечение разграничения и контроля доступа пользователей различными способами.</p> <p>4.1 Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin.</p> <p>4.2 Обеспечение разграничения и контроля доступа пользователей к техническим средствам вычислительной сети, на которых будет обрабатываться информация с использованием изделий семейства АПМДЗ «КРИПТОН-ЗАМОК».</p>	
Б1.Б.33	<p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» является ознакомление обучающихся с основными подходами анализа безопасности сложных систем, со средствами защиты информации, используемыми в составе АС в защищенном исполнении; в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p>	<p><i>Общая трудоемкость дисциплины составляет 9 зачетных единиц</i></p> <p>324</p> <p><i>акад.</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Дисциплина Разработка и эксплуатация защищенных автоматизированных систем входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Основы информационной безопасности</p> <p>Программно-аппаратные средства обеспечения информационной безопасности</p> <p>Организационное и правовое обеспечение информационной безопасности</p> <p>Методы выявления нарушений информационной безопасности, аттестация АИС</p> <p>Безопасность сетей ЭВМ</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Информационная безопасность распределенных информационных систем</p> <p>Анализ рисков информационной безопасности</p> <p>Управление информационной безопасностью</p> <p>Производственная-преддипломная практика</p> <p>Подготовка к сдаче и сдача государственного экзамена</p> <p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Разработка и эксплуатация защищенных автоматизированных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <p>понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем</p> <p>основные принципы построения защищенных распределенных компьютерных систем</p> <p>документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах.</p> <p>современные принципы построения архитектуры ИС.</p>	<p><i>часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Уметь осуществлять анализ несложных процессов проектирования применять государственные стандарты при проектировании автоматизированных систем в защищенном исполнении разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов</p> <p>Владеть 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</p> <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;</p> <p>Уметь осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы применять новые информационные технологии в сфере защиты данных</p> <p>Владеть методами исследования новых образцов программных, технических средств и информационных технологий, применяемых в области информационной безопасности</p> <p>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p>Знать • уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий;</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> • требования к разработке и производству, проведению испытаний, поддержке безопасности СЗИ для определения уровня доверия • положение о системе сертификации средств защиты информации; • продукцию, которую необходимо сертифицировать; • состав участников системы сертификации и их основные функции; • этапы сертификации; • требования к защищенности информации в автоматизированных системах; • требования к проведению испытаний СЗИ; • порядок проведения сертификационных испытаний. <p>Уметь</p> <ul style="list-style-type: none"> • составлять техническое задание на выполнение работ по проведению сертификационных испытаний; • составлять акт отбора образца; • подать заявку на сертификацию; • оформить экспертное заключение и проект сертификата соответствия по результатам сертификации. <p>Владеть</p> <ul style="list-style-type: none"> • навыками проведения испытаний средств защиты информации, а также обеспечения безопасности средств защиты информации в ходе их применения <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Защищенные автоматизированные системы. Основные понятия и классификация <ol style="list-style-type: none"> 1.1 Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. Современные принципы построения архитектуры АИС. 2. Разработка защищенных АС <ol style="list-style-type: none"> 2.1 Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении (АСЗИ). Последовательность и содержание этапов разработки АС. Формирование требований к АСЗИ. 2.2 Методы, способы и средства обеспечения отказоустойчивости АСЗИ 2.3 Разработка АСЗИ. Выбор мер защиты информации для реализации в АС 3. Основы эксплуатации защищенных АС <ol style="list-style-type: none"> 3.1 Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. 3.2 Анализ защищенности АС 3.3 Организация технического обслуживания защищённых АС. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.</p> <p>4. Основы администрирования АС</p> <p>4.1 Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования.</p> <p>5. Безопасность критической информационной инфраструктуры РФ</p> <p>5.1 ФЗ от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Субъекты КИИ. Значимые объекты КИИ. Категорирование объектов КИИ. Обеспечения безопасности объектов КИИ.</p> <p>5.2 Указ президента №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Функции центров ГосСОПКА. Правила эксплуатации центров ГосСОПКА. Построения собственного центра ГосСОПКА.</p> <p>6. Сертификации средств защиты информации автоматизированных систем</p> <p>6.1 Положение о системе сертификации средств защиты информации. Состав участников системы сертификации и их основные функции</p> <p>6.2 Руководящие нормативные и методические документы в системе сертификации средств защиты информации. Сертификация автоматизированных систем, средств вычислительной техники, межсетевых экранов, программного обеспечения.</p> <p>6.3 Требования по безопасности информации. Уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий</p> <p>6.4 Порядок сертификационных испытаний. Подготовка к проведению сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК России</p>	
Б1.Б.34	<p>Управление информационной безопасностью</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями изучения дисциплины «Управление информационной безопасностью» являются: формирование знаний принципов политики информационной безопасности в информационных системах; навыков организации и методологии обеспечения информационной безопасности автоматизированных систем, функционирующих на предприятиях и организациях РФ; умений по разработке нормативных материалов, регламентирующих работу по защите информации</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Управление информационной безопасностью входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения),</p>	<p><i>Общая трудоемкость дисциплины составляет 8 зачетных единиц</i></p> <p>288</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>сформированные в результате изучения дисциплин/ практик: Организационное и правовое обеспечение информационной безопасности Основы информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Производственная-преддипломная практика Подготовка к защите и защита выпускной квалификационной работы</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Управление информационной безопасностью» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней. <p>ПК-12 способностью участвовать в проектировании системы</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>управления информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ. <p>Владеть</p> <ul style="list-style-type: none"> - навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. <p>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. <p>ПК-28 способностью управлять информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>в ИС; - основные меры по ЗИ в АС. 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. ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>Знать - основы законодательства Российской Федерации; - нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - меры правовой и дисциплинарной ответственности за разглашение защищаемой информации. 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. ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p> <p>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. Уметь - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;</p> <p>- разрабатывать частные политики ИБ АС;</p> <p>- контролировать эффективность принятых мер по реализации частных политик ИБ АС.</p> <p>Владеть</p> <p>- навыками выявления угроз безопасности информации в АС;</p> <p>- владеть навыками разработки политик безопасности различных уровней.</p> <p>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах</p> <p>Знать</p> <p>Ключевые процессы менеджмента ИБ</p> <p>Требования нормативно-правовых документов, регламентирующих систему менеджмента информационной безопасности (СМИБ)</p> <p>Уметь</p> <p>Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации</p> <p>Определять цели применения мер и средств контроля и управления для обработки рисков</p> <p>Владеть</p> <p>Навыками выбора необходимых мер и средств контроля и управления ИБ</p> <p>Навыками определения способов измерения результативности выбранных мер управления ИБ</p> <p>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении</p> <p>Знать</p> <p>Этапы построения и использования СМИБ</p> <p>Семейство стандартов ISO/IEC 27000</p> <p>Уметь</p> <p>Оценивать уровень знаний сотрудников в области ИБ</p> <p>Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ</p> <p>Выявлять возможности улучшения СМИБ</p> <p>Владеть</p> <p>Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Создание системы управления информационной безопасностью</p> <p>1.1 Основные принципы создания системы управления информационной безопасностью. Структура системы управления информационной безопасностью</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.2 Проектирование систем ИБ. Внедрение ISO 27001/17799.</p> <p>1.3 Административный уровень обеспечения ИБ. Политики среднего и нижнего уровня.</p> <p>1.4 Разработка политик ИБ. Профиль защиты. Разработка профилей защиты и заданий по безопасности</p> <p>1.5 Расследование инцидентов ИБ. Администратор безопасности.</p> <p>1.6 Комплект типовых документов по ИБ.</p> <p>1.7 Технические политики ИБ.</p> <p>2. Обеспечение безопасности информации объектов КИИ</p> <p>2.1 Основные программно-технические подсистемы СОБИ КСИИ</p> <p>2.2 Управление ОБИ КСИИ документирование и реализация основных процессов.</p> <p>2.3 Этапы разработки СОБИ КИИ. Аналитическое обоснование необходимости создания СОБИ КИИ. Нормативные методические документы ФСТЭК России</p> <p>2.4 Техническое задание на разработку СОБИ КИИ. Основные проектные документы. Разработка комплекса внутренних организационно-распорядительных документов</p> <p>2.5 DLP-системы. Сравнение систем. Принципы создания</p>	
Б1.Б.35	<p>Инженерная графика</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины (модуля) «Инженерная графика» являются:</p> <ul style="list-style-type: none"> - овладение студентами знаниями, умениями и навыками, необходимыми для выполнения и чтения чертежей различного назначения и решения на чертежах инженерно-графических задач; - овладение решением задач геометрического моделирования и применения интерактивных графических систем для выполнения и редактирования изображений и чертежей; - овладение достаточным уровнем общепрофессиональной компетенции в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем. <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Инженерная графика входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: школьные курсы черчения, геометрии, информатики.</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Подготовка к защите и защита выпускной квалификационной работы</p> <p>3 Компетенции обучающегося, формируемые в результате</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы 108 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Инженерная графика» обучающийся должен обладать следующими компетенциями: ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> <p>Знать</p> <ul style="list-style-type: none"> - основные определения и понятия инженерной графики; - основные правила выполнения чертежей; - основные положения ЕСКД; - нормативные и руководящие материалы, касающиеся выполняемых типов чертежей <p>Уметь</p> <ul style="list-style-type: none"> - 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 <p>Владеть</p> <ul style="list-style-type: none"> - 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 <p>1. Единая система конструкторской документации. 1.1 Тема. Общие правила выполнения чертежей. Единая система конструкторской документации (ЕСКД). ГОСТ 2.301-68 Форматы. ГОСТ 2.302-68 Масштабы. ГОСТ 2.303-68 Линии чертежа. ГОСТ 2.304-81 Шрифты чертежные. ГОСТ 2.305-08. 1.2 Тема. ГОСТ 2.305-08 Изображения: виды, разрезы, сечения. ГОСТ 2.306-68 Обозначения графические материалов и правила их нанесения на чертежах. ГОСТ 2.307-2011. Нанесение размеров на чертежах и предельных отклонений.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.3 Тема. ГОСТ 2.702-2011 Правила выполнения электрических схем</p> <p>2. Основы начертательной геометрии.</p> <p>2.1 Тема. Методы проецирования. Комплексный чертеж в трех проекциях. Абсолютные и относительные координаты точки.</p> <p>2.2 Тема. Проекция прямой линии. Положение прямой в пространстве. Взаимное расположение прямых. Конкурирующие точки. Определение натуральной величины отрезка прямой методом прямоугольного треугольника. Проекция прямого угла.</p> <p>2.3 Тема. Плоскость. Элементы определяющие плоскость. Различные случаи положения в пространстве. Взаимное положение и принадлежность точек, прямых, плоскостей. Горизонтали, фронталы в плоскостях уровня, проецирующих и общего положения.</p> <p>2.4 Тема. Поверхности. Образование и задание поверхности на чертеже. Точка и линия принадлежащие поверхности. Сечение многогранников плоскостью частного и общего положения. Пересечение тел вращения плоскостью (цилиндр, конус, сфера).</p> <p>3. Аксонометрические проекции.</p> <p>3.1 Тема. Условия наглядности. Свойства параллельного проецирования. ГОСТ 2.317-2011 Стандартные виды аксонометрических проекций. Коэффициенты искажения. Построение плоских фигур и окружностей в различных видах аксонометрических проекций.</p> <p>4. Машиностроительное черчение.</p> <p>4.1 Тема. Резьбовые и сварные соединения. Элементы резьбы. Типы резьб. Изображение и обозначение резьбы.</p> <p>4.2 Тема. Сборочный чертеж, чертеж общего вида. Условности и упрощения при выполнении СЧ. Спецификация.</p> <p>Дисциплина включает в себя следующие разделы:</p>	
Б1.Б.36	<p>Информационная безопасность распределенных информационных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Информационная безопасность распределенных информационных систем» является систематизация и обобщение у обучающихся понятий о методах анализа угроз и уязвимостей, проектируемых и эксплуатируемых распределенных информационных систем, моделей угроз и нарушителя информационной безопасности распределенных информационных систем, получение практических навыков проектирования средств защиты информации в распределенных информационных системах, построения распределенных информационных систем.</p> <p>Овладение обучающимися необходимым и достаточным уровнем</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Информационная безопасность распределенных информационных систем входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Введение в специальность</p> <p>Основы информационной безопасности</p> <p>Организация ЭВМ и вычислительных систем</p> <p>Технологии и методы программирования</p> <p>Безопасность систем баз данных</p> <p>Языки программирования</p> <p>Сети и системы передачи информации</p> <p>Технология построения защищенных распределенных приложений</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>Научно-исследовательская работа</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Информационная безопасность распределенных информационных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-3 способностью проводить анализ защищенности автоматизированных систем</p> <p>Знать</p> <p>Критерии оценки эффективности и надежности средств защиты распределенных информационных систем (РИС).</p> <p>Принципы построения и функционирования распределенных информационных систем в защищённом исполнении.</p> <p>Методики анализа и контроля защищенности РИС в защищённом исполнении.</p> <p>Уметь</p> <p>Анализировать техническую и сопроводительную документацию по обеспечению ИБ.</p> <p>Анализировать программные и архитектурно-технические решения компонентов автоматизированных систем в защищённом исполнении.</p> <p>Проводить выбор технических, программно–аппаратных и</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>криптографических компонентов автоматизированных систем с целью совершенствования защиты.</p> <p>Владеть</p> <p>Навыками анализа основных узлов автоматизированных систем.</p> <p>Навыками анализа основных узлов автоматизированных систем в защищённом исполнении.</p> <p>Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении.</p> <p>ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <p>Основы организационного и правового обеспечения ИБ.</p> <p>Основные нормативные и правовые акты в области обеспечения ИБ.</p> <p>Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ.</p> <p>Методики проектирования АС в защищенном исполнении.</p> <p>Уметь</p> <p>Реализовывать разработанную автоматизированную систему с учетом требований ИБ.</p> <p>Организовывать реализацию разработанной АС с учетом требований информационной безопасности.</p> <p>Готовить сопроводительную документацию к разработанной АС в защищенном исполнении.</p> <p>Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.</p> <p>Владеть</p> <p>Навыками разработки автоматизированных систему с учетом требований ИБ.</p> <p>Навыками контроля разработки АС с учетом требований ИБ.</p> <p>Навыками контроля эффективности применения разработанной АС в защищенном исполнении.</p> <p>Навыками разработки сопроводительной документации к разработанной АС в защищенном исполнении</p> <p>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы</p> <p>Знать</p> <p>Принципы построения современных защищенных распределенных АС.</p> <p>Способы разработки политики безопасности распределенных ИС.</p> <p>Нормативные документы по стандартизации и сертификации</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>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. 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. ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами 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. 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.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать</p> <p>Основные принципы организации программных и программно-аппаратных СЗИ.</p> <p>Основные подходы создания программных и программно-аппаратных СЗИ.</p> <p>Основные подходы и способы реализации СКЗИ.</p> <p>Уметь</p> <p>Проводить комплексное тестирование и отладку программных и программно-аппаратных СЗИ.</p> <p>Администрировать программные и программно-аппаратные СЗИ.</p> <p>Проводить комплексное тестирование и отладку СКЗИ.</p> <p>Администрировать СКЗИ.</p> <p>Владеть</p> <p>Навыками комплексного тестирования и отладки программных и программно-аппаратных систем защиты информации.</p> <p>Навыками администрирования программных и программно-аппаратных СЗИ.</p> <p>Навыками комплексного тестирования и отладки СКЗИ.</p> <p>Навыками администрирования СКЗИ.</p> <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <p>Основные положения методики моделирования угроз безопасности информации</p> <p>Основные положения базовой модели угроз безопасности ПДн при их обработке в ИС ПДн</p> <p>Уметь</p> <p>Применять методику моделирования угроз безопасности информации для разработки частных моделей угроз и нарушителя</p> <p>Применять базовую модель угроз безопасности ПДн для разработки частных моделей угроз и нарушителя ИС ПДн</p> <p>Владеть</p> <p>Навыками классификации угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных</p> <p>Навыками разработки частных моделей угроз безопасности информации</p> <p>ПСК-7.3 способностью проводить аудит защищенности информационно-технологических ресурсов распределенных</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационных систем</p> <p>Знать</p> <p>Принципы организации распределенных корпоративных ИС. Основные этапы аудита информационной безопасности. Основные мероприятия при проведении аудита защищенности ИС</p> <p>Уметь</p> <p>Определять порядок организации информационного обмена между структурными подразделениями Обследовать системы на предмет наличия уязвимостей</p> <p>Владеть</p> <p>Методами оценки соблюдения требований стандартов и законов, на соответствие которым проводится аудит Навыками проведения инструментального анализа защищенности (оценка достаточности имеющихся и используемых на предприятии программных и технических СЗИ и полноты их использования)</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Методика построения системы ИБ предприятия</p> <p>1.1 Определение сведений, представляющих для организации интеллектуальную собственность. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них. Этапы формирования Перечня</p> <p>1.2 Методика определения границ обеспечения ИБ</p> <p>1.3 Анализ рисков</p> <p>1.4 Методика выбора контрмер, обеспечивающих ИБ объекта</p> <p>1.5 Методика выбора варианта ЗИ, в наибольшей степени удовлетворяющий заказчика. Математические методы оценки эффективности гипотетической СЗИ</p> <p>1.6 Принципы разработки пакета планирующих документов по построению системы ИБ, с помощью и на основе которого реализуется принятая политика ИБ</p> <p>2. Методики проведения мониторинга и аудита безопасности автоматизированной системы по требованиям безопасности информации</p> <p>2.1 Стандарты, используемые при проведении аудита безопасности информационных систем. Виды аудита информационной безопасности</p> <p>2.2 Этапы работ по проведению мониторинга и аудита безопасности автоматизированных информационных систем</p> <p>2.3 Перечень документации на АИС.</p> <p>2.4 Подходы к анализу данных мониторинга и аудита</p> <p>2.5 Методика формирования рекомендаций, выдаваемые аудитором по результатам анализа состояния ИС</p> <p>2.6 Структура отчета по результатам аудита безопасности ИС и анализу рисков</p> <p>2.7 Обзор программных продуктов, предназначенных для анализа и</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>управления рисками.</p> <p>3. Коммуникация в распределенных информационных системах, проектирование системы защиты информации в распределенных информационных системах</p> <p>3.1 Организация безопасности сетевых подключений распределенных информационных систем.</p> <p>3.2 Сложные распределенные системы-сферы применения</p> <p>3.3 Централизованная и децентрализованная модель организации распределенных информационных систем</p> <p>3.4 Этапы работ по проектированию системы ИБ.</p> <p>3.5 Перечень работы по внедрению системы ЗИ</p>	
Б1.Б.37	<p>Методы проектирования защищенных распределенных информационных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями изучения дисциплины «Методы проектирования защищенных распределенных информационных систем» являются: освоение моделей управления, получение знаний о закономерностях и свойствах процессов управления распределенными объектами, систематическое изучение основ теории и практики математического и имитационного моделирования систем; изучение основных подходов и математических схем к построению имитационных моделей; изучение возможностей применения имитационных моделей; освоение методологий и актуальных CASE-средств для имитационного моделирования систем и процессов в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Методы проектирования защищенных распределенных информационных систем входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Технология построения защищенных распределенных приложений</p> <p>Математическое моделирование распределенных систем</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа</p> <p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>Производственная-преддипломная практика</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i></p> <p>144</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Методы проектирования защищенных распределенных информационных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> — 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; <p>Уметь</p> <ul style="list-style-type: none"> — 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; <p>Владеть</p> <ul style="list-style-type: none"> — 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 <p>ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — 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 <p>Уметь</p> <ul style="list-style-type: none"> — разрабатывать и анализировать проектные решения по 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обеспечению безопасности автоматизированных систем; — применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем</p> <p>Владеть</p> <p>— 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</p> <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать</p> <p>— принципы построения и функционирования, примеры реализаций распределенных систем; — принципы работы элементов и функциональных узлов электронной аппаратуры; — концепции построения распределенных информационных систем</p> <p>Уметь</p> <p>— 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 — методикой эксплуатации современные программных, технических средств и информационных технологий; — навыками обеспечения безопасности информации с помощью типовых программных средств;</p> <p>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p> <p>Знать</p> <p>— нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; — 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;</p> <p>Уметь</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</p> <p>— разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;</p> <p>— разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем</p> <p>Владеть</p> <p>— 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;</p> <p>— нормативными требованиями по защите информации;</p> <p>— навыками организации и обеспечения режима секретности</p> <p>Дисциплина включает в себя следующие разделы</p> <p>1. Введение в распределенные системы</p> <p>1.1 Определение распределенной системы. Концепции аппаратных решений. Концепции программных решений. Модель клиент-сервер</p> <p>2. Связь и процессы в распределенных системах</p> <p>2.1 Уровни протоколов. Удаленный вызов процедур. Обращение к удаленным объектам.</p> <p>2.2 Связь по средством сообщений. Связь на основе потоков данных.</p> <p>2.3 Потоки выполнения задач. Пользовательские интерфейсы. Серверы объектов</p> <p>3. Синхронизация компонент в распределённых системах</p> <p>3.1 Синхронизация часов. Логические часы.</p> <p>3.2 Глобальное состояние. Алгоритмы голосования. Взаимное исключение.</p> <p>3.3 Распределенные транзакции</p> <p>4. Непротиворечивость и репликация в распределенных системах</p> <p>4.1 Модели непротиворечивости, ориентированные на данные. Модели непротиворечивости, ориентированные на клиента.</p> <p>4.2 Протоколы распределения. Протоколы реплицируемой записи. Протоколы согласования кэшей.</p> <p>5. Защищенность распределенных систем</p> <p>5.1 Защищенные каналы. Аутентификация. Целостность и конфиденциальность сообщений. Защищенное групповое взаимодействие.</p> <p>5.2 Контроль доступа. Брандмауэры. Защита мобильного кода.</p> <p>5.3 Управление защитой. Управление ключами. Управление</p> <p>6. Экзамен</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
Б1.Б.38	<p>Технология построения защищенных распределенных приложений</p> <p>1 Цели освоения дисциплины (модуля) Целями освоения дисциплины «Технология построения защищенных распределенных приложений» является формирование у обучающихся понятий о современных подходах к проектированию и построению, эксплуатации и модернизации защищенного программного обеспечения в целом, формирует у обучающихся системные представления о каноническом, автоматизированном, типовом подходе к проектированию распределенного программного обеспечения с применением современных CASE-средств, методах тестирования программного обеспечения, методах защиты программного обеспечения, формирует у обучающихся практические навыки использования CASE-средств для построения и модернизации программного обеспечения.</p> <p>Овладение обучающимися необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Технология построения защищенных распределенных приложений входит в базовую часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Организация ЭВМ и вычислительных систем Информатика Технологии и методы программирования Языки программирования Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Информационная безопасность распределенных информационных систем Методы проектирования защищенных распределенных информационных систем Анализ безопасности программного обеспечения</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Технология построения защищенных распределенных приложений» обучающийся должен обладать следующими компетенциями: ПК-13 способностью участвовать в проектировании средств</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i> 108 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>защиты информации автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - 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; <p>Владеть</p> <ul style="list-style-type: none"> - навыками оформления программной документации по ЕСПД; ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - навыками разработки приложений на языке C# с применением многопоточности; - навыками разработки приложений на языке LabVIEW с применением многопоточности; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - варианты интерпретации бинарного потока данных; - структуру пакетов данных транспортного уровня протокола ТСР; <p>Уметь</p> <ul style="list-style-type: none"> - выполнять анализ данных транспортного уровня протокола ТСР при помощи специализированного программного обеспечения; <p>Владеть</p> <ul style="list-style-type: none"> -навыками сериализации данных; <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Введение в распределенные приложения</p> <p>1.1 Понятие распределенного приложения. Определение распределенного приложения. Программные компоненты. Требования к распределенным приложениям. Понятие промежуточной среды.</p> <p>1.2 Программные конструкции языка С# и функции платформы .NET необходимые для реализации простейших сетевых приложений.</p> <p>1.3 Функционал среды разработки LabVIEW и платформы Run-Time Engine необходимый для реализации сетевых приложений.</p> <p>2. Методы организации обмена данными в распределенном приложении</p> <p>2.1 Применение удаленного вызова процедуры. Применение удалённого вызова метода. Применение очередей сообщений. Синхронный и асинхронный обмен данными</p> <p>3. Особенности применения клиент/серверной архитектуры при построении распределенных приложений</p> <p>3.1 Применение многопоточности при построении серверной части распределенного приложения. Реализация на С# и в LabVIEW. Сериализация данных. Реализация на С# и в LabVIEW. Кроссплатформенное распределенное программное</p> <p>4. Криптографические протоколы обмена информацией.</p> <p>4.1 Применение SSL и SSH для организации защищенного обмена данными. Разработка приложений использующих SSL и SSH на языке С# и в LabVIEW.</p>	
Б1.Б.39	<p>Введение в специальность</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Введение в специальность » является ознакомление обучающихся с профессиональной деятельностью в сфере разработки, исследования и эксплуатации систем обеспечения информационной безопасности автоматизированных</p>	<p><i>Общая трудоемкость дисциплины составл</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>систем в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Введение в специальность» содействует формированию мировоззрения и системного мышления, ориентирует обучающихся в широкой сфере проблем обеспечения информационной безопасности автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Введение в специальность входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Дисциплина «Введение в специальность» входит в базовую часть блока 1 образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения «Информатика и информационно-коммуникационные технологии», «Алгебра» и «Физика» в объеме средней общеобразовательной школы.</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Основы информационной безопасности</p> <p>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Введение в специальность» обучающийся должен обладать следующими компетенциями:</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> • политику государства в области обеспечения информационной безопасности • национальные, межгосударственные и международные стандарты 	<p><i>лет 2</i></p> <p><i>зачетных</i></p> <p><i>единиц</i></p> <p><i>72 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>в области защиты информации</p> <ul style="list-style-type: none"> • современное состояние рынка труда в области обеспечения информационной безопасности • профессиональный стандарт «Специалист по защите информации в автоматизированных системах» • трудовое законодательство РФ <p>Уметь</p> <ul style="list-style-type: none"> • анализировать информацию по вопросам национальной и информационной безопасности государства; • соблюдать нормы профессиональной этики <p>Владеть</p> <ul style="list-style-type: none"> • профессиональной терминологией в области информационной безопасности; • практическими навыками соблюдения норм профессиональной этики. <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> • Основы построения систем обработки и передачи информации, их современное состояние развития. • Основные задачи обеспечения безопасности информации в компьютерных и автоматизированных системах. • Особенности обработки информации с использованием компьютерных систем <p>Уметь</p> <ul style="list-style-type: none"> • Осуществлять поиск и систематизировать современную научно-техническую информацию по рассматриваемым вопросам в рамках дисциплины. • Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам. <p>Владеть</p> <ul style="list-style-type: none"> • Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам. • Навыками осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Доктрина информационной безопасности <ol style="list-style-type: none"> 1.1 Общие положения. Основные информационные угрозы и состояние информационной безопасности. 1.2 Стратегические цели и основные направления обеспечения информационной безопасности 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> 2. Организационная основа системы обеспечения информационной безопасности <ul style="list-style-type: none"> 2.1 Деятельность государственных органов по обеспечению информационной безопасности. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности. Задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности 3. Национальные интересы РФ в информационной сфере <ul style="list-style-type: none"> 3.1 Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры 3.2 Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, в области обеспечения информационной безопасности 4. Способы нарушения информационной безопасности <ul style="list-style-type: none"> 4.1 Классификация способов нарушения информационной безопасности 4.2 Способы противодействия нарушению информационной безопасности 5. Информационные войны <ul style="list-style-type: none"> 5.1 Классификация и способы информационной войны. Объекты воздействия. Источники угроз. Анализ риска информационной войны 6. Криптография и стеганография <ul style="list-style-type: none"> 6.1 Классическая, компьютерная и цифровая стеганография. Атаки на стегосистемы. Применение стеганографии 6.2 Криптография и криптоанализ. Криптографические методы. Основные проблемы криптографии. Законодательство в области криптографии и стеганографии. 7. Технические каналы утечки информации <ul style="list-style-type: none"> 7.1 Причины утечек данных и возможные ситуации. Классификация технических каналов утечки информации. Использование технических каналов утечки информации 7.2 Средства и системы для обнаружения утечки информации. Способы защиты информации 	
Б1.Б.40	Продвижение научной продукции. 1 Цели освоения дисциплины (модуля)	<i>Общая трудоем</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- развитие у студентов личностных качеств, а также формирование общекультурных и общепрофессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем;</p> <p>- формирование у студентов представлений о видах научной продукции и путях продвижения ее на рынок, получение комплекса знаний о системе государственной поддержки, грантах, фондах и оформлении конкурсной документации;</p> <p>- освоение студентами навыков проведения патентного поиска, оформления патентной документации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Продвижение научной продукции входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Экономика Правоведение История</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа Основы управленческой деятельности Подготовка к сдаче и сдача государственного экзамена Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Подготовка к защите и защита выпускной квалификационной работы Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Продвижение научной продукции» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-8 способностью к самоорганизации и самообразованию</p> <p>Знать</p> <p>- порядок и особенности выполнения научно-исследовательских работ по государственным контрактам;</p> <p>- отличительные признаки инновационной продукции.</p> <p>Уметь</p> <p>- приобретать знания в области продвижения научной продукции;</p> <p>- определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных</p>	<p><i>кость дисциплины составляет 3 зачетных единицы 108 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>технологий, глобальный информационный ресурсов.</p> <p>Владеть</p> <ul style="list-style-type: none"> - классификацией научно-технической продукции, профессиональным языком в области продвижения научной продукции; - практическими навыками оценки качества для научно-технической продукции, навыками составления конкурсной документации. <p>ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> <p>Знать</p> <ul style="list-style-type: none"> - средства и методы стимулирования сбыта продукции. Виды охранных документов интеллектуальной собственности; - основные шаги и правила государственной системы регистрации результатов научной деятельности. <p>Уметь</p> <ul style="list-style-type: none"> - составлять пакет документов для регистрации программы ЭВМ; - составлять пакет документов для регистрации изобретения или полезной модели. <p>Владеть</p> <ul style="list-style-type: none"> - способами анализа патентной документации и проведения патентного поиска; - способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды. <p>ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - систему финансирования инновационной деятельности в различных сферах жизнедеятельности; - принципы, формы и методы финансирования научно-технической продукции; - средства и методы стимулирования сбыта продукции. <p>Уметь</p> <ul style="list-style-type: none"> - 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; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов.</p> <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - основные виды охранных документов интеллектуальной собственности; - ключевые этапы и правила государственной системы регистрации результатов научной деятельности; - формы государственной поддержки инновационной деятельности в России. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - вопросами правового регулирования деятельности предприятия; - знаниями о научно-технической политике России; - навыками составления конкурсной документации. <p>Дисциплина включает в себя следующие разделы:</p> <p>1.1 Научно-техническая продукция. Общие сведения. Термины и определения предметной области знаний.</p> <p>1.2 Рынок научно-технической продукции: участники, особенности, коммерческие и некоммерческие способы продвижения результатов научно-исследовательской и инновационной деятельности на рынок.</p> <p>1.3 Анализ рисков при продвижении результатов научно-исследовательской и инновационной деятельности на рынок. Виды рисков и способы управления.</p> <p>1.4 Патентная охрана результатов интеллектуальной деятельности. Патентные исследования. Механизмы передачи прав на объекты</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>интеллектуальной собственности.</p> <p>1.5 Инновации: подходы к определению, классификация и источники возникновения. Факторы, сдерживающие процесс создания инноваций в России.</p> <p>1.6 Инновационный процесс. Основные особенности и этапы инновационного процесса.</p> <p>1.7 Экспертиза инновационных проектов.</p> <p>Понятие и критерии коммерциализуемости инновационного проекта.</p> <p>1.8 Основы бизнес-планирования.</p> <p>1.9 Формы и источники финансирования научно-исследовательской и инновационной деятельности.</p>	
Б1.Б.41	<p>Физическая культура и спорт</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью освоения дисциплины «Физическая культура и спорт» является формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта для сохранения и укрепления здоровья, а также подготовка к будущей профессиональной деятельности.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Физическая культура и спорт входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Адаптивные курсы по физической культуре и спорту Элективные курсы по физической культуре и спорту Безопасность жизнедеятельности</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Элективные курсы по физической культуре и спорту Подготовка к сдаче и сдача государственного экзамена Адаптивные курсы по физической культуре и спорту</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Физическая культура и спорт» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-9 способностью использовать методы и средства физической</p>	<p><i>Общая трудоемкость дисциплины составляет 2 зачетных единицы 72 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>культуры для обеспечения полноценной социальной и профессиональной деятельности</p> <p>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.</p> <p>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.</p> <p>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</p> <p>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</p> <p>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.</p> <p>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.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <p>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.</p> <p>ОПК-7 способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 <p>Уметь</p> <ul style="list-style-type: none"> - выделять основные опасности среды обитания человека; - оценивать риск их реализации <p>Владеть</p> <ul style="list-style-type: none"> - основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций <p>Дисциплина включает в себя следующие разделы:</p> <p>Раздел 1 Физическая культура в общекультурной и профессиональной подготовке студентов</p> <p>1.1 Физическая культура личности. Основные понятия и определения в области физической культуры. Компоненты физической культуры, ее социальные функции. Уровни сформированности физической культуры личности</p> <p>2. Раздел 2 Организационные и методические основы физического воспитания</p> <p>2.1 Методические принципы физического воспитания. Методы и средства физического воспитания. Методики воспитания физических качеств. Профессионально-прикладная физическая подготовка. Техника безопасности на занятиях физической культурой</p> <p>3. Раздел 3 Анатомо-морфологические и физиологические основы жизнедеятельности организма человека при занятиях физической культурой</p> <p>3.1 Организм как единая саморазвивающаяся и</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>саморегулирующаяся биологическая система. Внешняя среда и ее воздействие на организм и жизнедеятельность человека. Функциональная активность человека. Биологические ритмы и работоспособность</p> <p>4. Раздел 4 Основы здорового образа жизни студента</p> <p>4.1 Физическое здоровье и его критерии. Ценностные ориентации молодежи на здоровый образ жизни. Контроль и самоконтроль физического состояния.</p> <p>5.1 Виды спорта. Олимпийские игры. Комплекс ГТО в программе физического воспитания студентов (история, организация работы по совершенствованию физических качеств)</p>	
Б1.В	Вариативная часть	
Б1.В.ОД	Обязательные дисциплины	
Б1.В.01	<p>Иностранный язык в профессиональной деятельности</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Цели освоения дисциплины «Иностранный язык в профессиональной деятельности»: - повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени обучения;</p> <p>- овладение студентами необходимым и достаточным количеством общекультурных и профессиональных компетенций, направленных на формирование системы языковых знаний, умений и навыков практического владения иностранным языком в профессиональной сфере.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Иностранный язык в профессиональной деятельности входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Дисциплина «Иностранный язык в профессиональной деятельности» входит в вариативную часть образовательного стандарта специалиста Б1.В.01 «Иностранный язык в профессиональной деятельности».</p> <p>Для изучения дисциплины «Иностранный язык в профессиональной деятельности» необходимы знания, умения, навыки, сформированные в результате освоения дисциплины «Иностранный язык».</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Иностранный язык в профессиональной деятельности» обучающийся должен обладать</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i></p> <p>144</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>следующими компетенциями:</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - 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 перевода, его целей и условий осуществления. <p>Владеть</p> <ul style="list-style-type: none"> - 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). <p>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</p> <p>Знать</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>основные приемы и методы, связанные с поиском, изучением, обобщением и систематизацией научно-технической информации</p> <p>Уметь использовать основные приемы и методы для поиска, изучения, обобщения и систематизации научно-технической информации</p> <p>Владеть основными приемами и методами для поиска, изучения, обобщения и систематизации научно-технической информации</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Сфера будущей профессиональной деятельности</p> <p>1.1 Развитие умений и навыков письма по теме: «История развития профессии и профессиональной сферы»</p> <p>1.2 Развитие навыков чтения текстов по теме. «Современные технологии и перспективы развития профессии и профессиональной сферы»</p> <p>1.3 Развитие навыков говорения по теме «Мировые ведущие предприятия и компании профессиональной сферы»</p> <p>1.4 Развитие умений и навыков оперирования основными грамматическими явлениями, характерными для профессиональной речи. Категория «Залог»</p> <p>2. Моя будущая карьера.</p> <p>2.1 Развитие умений и навыков чтения, письма по теме «Основные сферы применения моей специальности. Охрана труда и рабочее место специалиста»</p> <p>2.2 Развитие навыков говорения «Профессиональные компетенции будущего специалиста»</p> <p>2.3 Развитие навыков письма по теме «Устройство на работу. Прохождение собеседования. Деловая этика»</p> <p>3. Основы профессиональной коммуникации</p> <p>3.1 Развитие навыков перевода профессиональной лексики, формул, метрических единиц</p> <p>3.2 Развитие навыков чтения и перевода текстов по специальности и деловой корреспонденции.</p> <p>3.3 Развитие навыков письма Аннотирование и реферирование текстов по специальности.</p>	
Б1.В.02	<p>Информационные технологии. Базы данных.</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Информационные технологии. Базы данных» является знакомство с моделями данных, используемыми в СУБД, изучение основ теории реляционных баз данных и методов проектирования баз данных, и формировании у обучающихся навыков их практического применения в соответствии с требованиями ФГОС ВО по направлению «Информационная</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетны</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>безопасность автоматизированных систем». Дисциплина «Информационные технологии. Базы данных» рассматривает основные подходы и методы проектирования реляционных баз данных и позволяет приобрести навыки практического использования СУБД реляционного типа, ее возможностей и особенностей.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Информационные технологии. Базы данных входит в вариативную часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Организация ЭВМ и вычислительных систем Информатика Языки программирования Основы информационной безопасности Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Безопасность систем баз данных Технологии и методы программирования Программно-аппаратные средства обеспечения информационной безопасности Технология построения защищенных распределенных приложений Информационная безопасность распределенных информационных систем Криптографические методы защиты информации Тестирование систем защиты информации автоматизированных систем Защита электронного документооборота</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Информационные технологии. Базы данных» обучающийся должен обладать следующими компетенциями:</p> <p>Структурный элемент компетенции</p> <p>Планируемые результаты обучения</p> <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать</p> <ul style="list-style-type: none"> – основные информационные технологии, используемые в автоматизированных системах; - основные программные и технические средства для безопасной 	<p>х единицы 180 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>работы с базой данных (БД);</p> <ul style="list-style-type: none"> - новые образцы программных, технических средств для БД; - системы управления базами данных; - способы и алгоритм внедрения и продуктивного использования новых программных, технических средств для БД; <p>Уметь</p> <ul style="list-style-type: none"> - 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; <p>Владеть</p> <ul style="list-style-type: none"> - навыками работы на языке манипулирования БД; - методами оценки правильности проектирования БД; <p>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - 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; <p>Владеть</p> <ul style="list-style-type: none"> - методиками безопасной работы с БД с помощью современных образцов программных, технических средств; - в полной мере средствами администрирования БД в интегрированных средах СУБД. <p>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - методологию и этапы проектирования базы данных; - метод «сущность-связь» для проектирования БД; - методы и подходы создания инфологической модели БД; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Уметь</p> <ul style="list-style-type: none"> -разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; - применять средства обеспечения безопасности баз данных; <p>Владеть</p> <ul style="list-style-type: none"> - основами проектирования БД; - навыками отображения предметной области на конкретную модель данных; <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Введение в базы данных. <ol style="list-style-type: none"> 1.1 БД и информационные системы. 1.2 Функции СУБД. Типовая организация СУБД. Основные функции СУБД. 2. Модели данных. <ol style="list-style-type: none"> 2.1 Понятие модели данных. Виды моделей. 2.2 Иерархические системы. Достоинства и недостатки. 2.3 Сетевые системы. Достоинства и недостатки. 3. Общие понятия реляционного подхода к организации БД. <ol style="list-style-type: none"> 3.1 Базовые понятия реляционных БД. Основные концепции и термины. 3.2 Основы реляционной алгебры и реляционного исчисления. 3.3 Теоретико-множественные операции реляционной алгебры. 4. Проектирование реляционных БД. <ol style="list-style-type: none"> 4.1 Инфологическое моделирование. Методики проектирования. 4.2 Проектирование реляционных баз данных с использованием нормализации. 4.3 Семантическое моделирование данных. Метод проектирования «Сущность-Связь». 4.4 Семантическое моделирование в современных CASE-системах. 5. Средства автоматизации проектирования. <ol style="list-style-type: none"> 5.1 Модели автоматизации проектирования. Средства автоматизации проектирования. 6. Язык SQL. <ol style="list-style-type: none"> 6.1 Функции, основные возможности. Синтаксис. 6.2 Операторы определения и манипулирования схемой БД. Типы SQL-запросов. 6.3 Определения ограничений целостности и триггеров. 7. Распределенная обработка данных. <ol style="list-style-type: none"> 7.1 Модели архитектуры «клиент-сервер». Управление распределенными данными. 7.2 Доступ к базам данных в двухзвенных моделях клиент-сервер. 8. Модели транзакций <ol style="list-style-type: none"> 8.1 Понятие транзакции. Две базовые модели транзакций: ANSI и расширенная модель транзакций. 9. Разработка БД В MS SQL Server 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>9.1 Язык описания данных DDL</p> <p>9.2 Создание таблиц для хранения данных. Использование команд DML для манипулирования данными.</p> <p>9.3 Применение представлений для просмотра и доступа к данным. Управление доступом к индивидуальным объектам базы данных.</p> <p>9.4 Написание многостолбцовых подзапросов</p> <p>Использование скалярных и коррелированных подзапросов</p> <p>Поддержка регулярных выражений в SQL.</p>	
Б1.В.03	<p>Моделирование угроз информационной безопасности</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины (модуля) «Моделирование угроз информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, разработка модели угроз с учетом различных факторов; исследование и оценка существующих моделей согласно требованиям стандартов информационной безопасности и нормативных документов ФСТЭК России.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Моделирование угроз информационной безопасности входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>Организационное и правовое обеспечение информационной безопасности</p> <p>Методы выявления нарушений информационной безопасности, аттестация АИС</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Анализ рисков информационной безопасности</p> <p>Моделирование систем и процессов защиты информации</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Моделирование угроз информационной безопасности» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать средства моделирования угроз информационной безопасности.</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i></p> <p>180</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Уметь применять языки, системы и инструментальные средства программирования для моделирования угроз информационной безопасности.</p> <p>Владеть навыками применения инструментальных средств программирования для моделирования угроз.</p> <p>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>Знать основные источники угроз ИБ; классификацию угроз информационной безопасности; Типовую модель угроз информационной безопасности Нормативно-методические документы в области моделирования угроз, способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах;</p> <p>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.</p> <p>Владеть Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; Навыками разработки частных моделей угроз</p> <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>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.</p> <p>Порядок разработки модели угроз</p> <p>Уметь оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные ресурсы</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>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. Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Введение <ol style="list-style-type: none"> 1.1 Цели и задачи моделирования угроз ИБ Нормативные и правовые акты в области защиты информации 2. Этапы моделирования угроз ИБ <ol style="list-style-type: none"> 2.1 Выявление объектов информационной системы подлежащих защите. Определение источников угроз 2.2 Наиболее часто реализуемые угрозы. Выявление способов реализации угроз 2.3 Угрозы мобильным устройствам. 3. Описание информационной системы <ol style="list-style-type: none"> 3.1 Угрозы за счет реализации ТКУИ 3.2 Методики построение дерева угроз 3.3 Разработка с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании 4. Модель угроз ИСПДн информационной системы персональных данных <ol style="list-style-type: none"> 4.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн. 4.2 Классификация угроз безопасности персональных данных по способу реализации 5. Основные законы распределения вероятностей для статистического моделирования угроз <ol style="list-style-type: none"> 5.1 Ошибки, возникающие при моделировании угроз. Определение вероятности возникновения отдельных угроз. Программные средства моделирования угроз 	
Б1.В.04	<p>Алгоритмы шифрования информации 1 Цели освоения дисциплины (модуля) Целями освоения дисциплины «Алгоритмы шифрования информации» является формирование у студентов понятий об основных методах шифрования, криптографических протоколах, базовых алгоритмах, применяемых в криптосистемах, алгоритмах шифрования с симметричным и несимметричным ключом. Овладение студентами необходимым и достаточным уровнем</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетны</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Алгоритмы шифрования информации входит в вариативную часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Математическая логика и теория алгоритмов Дискретная математика Теория информации Организация ЭВМ и вычислительных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Алгоритмы шифрования информации» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <p>Классификацию методов шифрования сообщений. Основы теории засекреченной связи. Математические операции, применяемые при шифровании данных.</p> <p>Уметь</p> <p>Применять алгоритмы блочного шифрования при разработке ПО. Применять алгоритмы симметричного шифрования при разработке ПО</p> <p>Владеть</p> <p>Навыками частотного анализа; Навыками применения метода полного перебора; Навыками атаки на закрытое и открытое сообщение.</p> <p>ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования,</p>	<p>х единицы 180 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать Системы блочного шифрования. Системы симметричного шифрования Хеш-функции; Протоколы обмена ключами.</p> <p>Уметь Реализовывать на языках высокого уровня алгоритмы шифров однозначной замены; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров; Реализовывать на языках высокого уровня алгоритмы омофонических шифров; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров.</p> <p>Владеть Навыками разработки защищенного программного обеспечения с применением шифров гаммирования; Навыками разработки защищенного программного обеспечения с применением комбинированных шифров; Навыками разработки защищенного программного обеспечения с применением шифров с открытым ключом;</p> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Введение в шифрование <ol style="list-style-type: none"> 1.1 Шифры замены и перестановки. Типы атак на примитивные шифры. 2. Симметричные криптографические системы <ol style="list-style-type: none"> 2.1 Блочные шифры. Составные шифры. Атаки на блочные шифры. 3. Поточковые шифры и генераторы ГСПЧ <ol style="list-style-type: none"> 3.1 Общие сведения. Принципы использования ГСПЧ. Классификация поточковых шифров. Шифр А5. Шифр RC4. 4. Блочное симметричное шифрование данных (DES) <ol style="list-style-type: none"> 4.1 Принципы построения алгоритма DES. Анализ алгоритма DES. Безопасность DES. 5. ГОСТ 28147-89 <ol style="list-style-type: none"> 5.1 Математический базис ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Безопасность ГОСТ 28147-89. 6. AES <ol style="list-style-type: none"> 6.1 Математический базис AES. Формат данных AES. Структура алгоритма и раундов AES. Стойкость AES 7. IDEA <ol style="list-style-type: none"> 7.1 Структура алгоритма IDEA. Шифрование данных IDEA. Безопасность IDEA. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
Б1.В.05	<p>Методы выявления нарушений информационной безопасности, аттестация АИС</p> <p>1 Цели освоения дисциплины (модуля) Целью дисциплины «Методы выявления нарушений информационной безопасности, аттестация АИС» является формирование профессиональных навыков аттестационных испытаний ОИ, изучение методик проведения аттестации, овладение методами мониторинга и аудита АС и подготовка к деятельности, связанной с аттестацией АИС в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Методы выявления нарушений информационной безопасности, аттестация АИС» рассматривает базовые теоретические понятия, средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Методы выявления нарушений информационной безопасности, аттестация АИС входит в вариативную часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Организация ЭВМ и вычислительных систем Введение в специальность Теория информации Информатика Языки программирования Теория вероятностей, математическая статистика Математический анализ Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Основы информационной безопасности Дискретная математика Теория графов и ее приложения Исследование операций и теория игр Математическая логика и теория алгоритмов Программно-аппаратные средства обеспечения информационной безопасности Математическое моделирование распределенных систем Безопасность систем баз данных Безопасность сетей ЭВМ Техническая защита информации Знания (умения, владения), полученные при изучении данной</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i> 180 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>дисциплины будут необходимы для изучения дисциплин/практик: Методы мониторинга информационной безопасности АС Моделирование угроз информационной безопасности Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Управление информационной безопасностью Анализ рисков информационной безопасности Методы проектирования защищенных распределенных информационных систем Информационная безопасность систем организационного управления Научно-исследовательская работа Моделирование систем и процессов защиты информации Подготовка к защите и защита выпускной квалификационной работы Производственная-преддипломная практика 3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Методы выявления нарушений информационной безопасности, аттестация АИС» обучающийся должен обладать следующими компетенциями: ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации 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. 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. ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем Знать — Источники и классификацию угроз информационной</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>безопасности;</p> <ul style="list-style-type: none"> — Основные принципы построения систем защиты информации; — Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. <p>Уметь</p> <ul style="list-style-type: none"> — Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; — Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; — Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем. <p>Владеть</p> <ul style="list-style-type: none"> — Методами выявления угроз информационной безопасности автоматизированных систем; — Методами аудита уровня защищенности АИС. <p>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; — Принципы администрирования системы информационной безопасности автоматизированной системы. <p>Уметь</p> <ul style="list-style-type: none"> — Настраивать систему информационной безопасности автоматизированной системы; — Настраивать подсистемы системы информационной безопасности автоматизированной системы; — Самостоятельно администрировать систему информационной безопасности автоматизированной системы. <p>Владеть</p> <ul style="list-style-type: none"> — Навыками работы с системой информационной безопасности автоматизированной системы; — Навыками работы с подсистемами системы информационной безопасности автоматизированной системы; — Навыками администрирования системы информационной безопасности автоматизированной системы. <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Общие положения проведения аттестационных испытаний <ol style="list-style-type: none"> 1.1 Предмет и содержание дисциплины. Методы проверок и испытаний. 1.2 Цели и задачи аттестационных испытаний. 2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте <ol style="list-style-type: none"> 2.1 Описание и классификация объектов информатизации. 2.2 Работы, выполняемые в ходе аттестационных испытаний АС. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>3. Методики проведения аттестации</p> <p>3.1 Методика проведения аттестации информационной системы по требованиям защиты персональных данных. Подготовка отчетной документации.</p> <p>3.2 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.</p> <p>4. Методика аттестационных испытаний выделенных помещений по требованиям безопасности информации</p> <p>4.1 Условия и порядок проведения аттестационных испытаний ВП.</p> <p>4.2 Объемы испытаний на соответствие требованиям по защите информации для ВП. Подготовка отчетной документации.</p> <p>5. Методы выявления нарушений ИБ</p> <p>5.1 Системы и методы обнаружения вторжений</p> <p>5.2 Способы построения «образа» нормального функционирования защищаемой системы. Определение общего показателя аномальности.</p> <p>5.3 Анализ методов обнаружения злоупотреблений. Базы сигнатур атак.</p>	
Б1.В.06	<p>Анализ рисков информационной безопасности</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины (модуля) «Анализ рисков информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, фиксация параметров безопасности и анализа безопасности АС, изучение основных понятий и принципов анализа и оценки рисков информационной безопасности.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Анализ рисков информационной безопасности входит в вариативную часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Моделирование угроз информационной безопасности</p> <p>Организационное и правовое обеспечение информационной безопасности</p> <p>Разработка и эксплуатация защищенных автоматизированных систем</p> <p>Методы выявления нарушений информационной безопасности, аттестация АИС</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа</p> <p>Производственная-преддипломная практика</p> <p>Подготовка к сдаче и сдача государственного экзамена</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i></p> <p>144 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Анализ рисков информационной безопасности» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - методологию анализа рисков информационной безопасности; - методики определения 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. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах; <p>Уметь</p> <ul style="list-style-type: none"> - оценивать информационные риски в автоматизированных 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>системах;</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем. <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Методики и технологии управления рисками информационной безопасности и их оценки</p> <p>1.1 Оценочные стандарты в информационной безопасности. Роль стандартов информационной безопасности. «Критерии определения безопасности компьютерных систем» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.</p> <p>1.2 Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей</p> <p>1.3 Методика оценки рисков информационной организации. Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность</p> <p>1.4 Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM</p> <p>1.5 Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам. Методика анализа рисков Microsoft</p> <p>1.6 Современные методы и средства анализа и управление рисками информационных систем. Методика FRAP. Методика OCTAVE. Методика RiskWatch</p>	
Б1.В.07	<p>Моделирование систем и процессов защиты информации</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью освоения дисциплины «Моделирование систем и процессов защиты информации» является формирование у обучающихся знаний по основам организации, управления и обеспечения безопасности и целостности данных информационных систем и технологий, а также навыков и умений в области анализа</p>	<p><i>трудоемкость дисциплины составляет 5 зачетны</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах, ознакомление с принципами моделирования систем и процессов защиты информации.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Моделирование систем и процессов защиты информации входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Информатика Основы информационной безопасности Информационные технологии. Базы данных Безопасность сетей ЭВМ Безопасность систем баз данных Безопасность операционных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к защите и защита выпускной квалификационной работы Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Моделирование систем и процессов защиты информации» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-2 способностью создавать и исследовать модели автоматизированных систем</p> <p>Знать</p> <p>основные принципы моделирования и виды моделей, требования, предъявляемые к моделям; методы оценки качества моделей, методы и средства моделирования; методы исследования моделей автоматизированных систем; структуру и состав автоматизированных систем управления.</p> <p>Уметь</p> <p>применять различные методы моделирования автоматизированных систем; выбирать методы и средства моделирования подсистем защиты информации; анализировать и оценивать угрозы информационной безопасности</p>	<p>х <i>единицы</i> 180 <i>акад.</i> <i>часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>объекта.</p> <p>Владеть</p> <p>навыками анализа информационной инфраструктуры автоматизированной системы;</p> <p>методами моделирования автоматизированных систем;</p> <p>основами построения моделей автоматизированных систем;</p> <p>навыками формализации задач и постановки задач моделирования;</p> <p>навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.</p> <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <p>нормативно-методическую основу моделирования угроз;</p> <p>методику моделирования угроз;</p> <p>цели и задачи моделирования систем и процессов защиты информации;</p> <p>этапы моделирования и виды моделей систем и процессов защиты информации; основные принципы построения моделей систем защиты информации;</p> <p>Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами;</p> <p>Базовую модель угроз безопасности ПДн;</p> <p>Классификацию угроз ПДн.</p> <p>Уметь</p> <p>обосновать выбор метода моделирования;</p> <p>исследовать модели информационно-технологических ресурсов объекта информатизации;</p> <p>составлять обобщенную модель системы защиты информации;</p> <p>разрабатывать модели угроз объекта информатизации;</p> <p>разрабатывать модели нарушителей информационной безопасности автоматизированных систем;</p> <p>применять различные методы моделирования систем защиты информации;</p> <p>описывать объект защиты;</p> <p>определять источники угроз;</p> <p>определять угрозы утечки информации по техническим каналам.</p> <p>Владеть</p> <p>приемами исследования процессов защиты информации в автоматизированных системах</p> <p>методами моделирования систем защиты информации</p> <p>навыками формирования списка уязвимостей объекта защиты</p> <p>навыками описания угроз безопасности</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>навыками анализа защищенности основных узлов и устройств современных автоматизированных систем</p> <p>навыками составления типовых моделей угроз безопасности персональных данных</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Моделирование систем и процессов защиты информации</p> <p>1.1 Математическое моделирование. Форма и принципы представления математических моделей</p> <p>Моделирование как метод научного исследования. Типы моделей.</p> <p>1.2 Компьютерное моделирование и вычислительный эксперимент. Генерация непрерывных и дискретных случайных величин: Генерация случайных процессов: основные подходы.</p> <p>1.3 Статистическое имитационное моделирование. Особенности имитационного моделирования. Этапы имитационного моделирования.</p> <p>1.4 Обобщенные модели систем защиты</p> <p>1.5 Моделирование систем защиты информации. Применение теории графов, теории игр, сетей Петри</p> <p>1.6 Методика моделирования угроз.</p> <p>Модель нарушителя</p> <p>1.7 Типовые модели угроз безопасности ПДн</p> <p>1.8 Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования.</p> <p>1.9 Подготовка к экзамену</p>	
Б1.В.ДВ.01	Дисциплины по выбору Б1.В.ДВ.01	
Б1.В.ДВ.01.01	<p>Основы радиотехники</p> <p>1. Цели освоения дисциплины</p> <p>Целью освоения дисциплины «Основы радиотехники» является формирование способности анализировать электромагнитные колебания радиодиапазона с применением соответствующего математического аппарата, способности применять знания в области электроники и схемотехники для генерации, усиления, излучения и приема, применения радиоволн для передачи на большие расстояния информации в радиосвязи, радио- и телевидении, радиолокации, радионавигации и радиоподавления, а также разработки программно-аппаратных компонентов защищенных автоматизированных систем.</p> <p>Эта цель достигается в ходе выполнения следующих задач:</p> <ul style="list-style-type: none"> – изучение основ излучения, распространения и приема радиоволн; – изучения передающих и приемных антенн различных диапазонов длин волн; – изучение методов формирования и преобразования 	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i></p> <p>180</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>сигналов;</p> <ul style="list-style-type: none"> – изучение принципов построения передающей и приемной аппаратуры; – изучение структурных схем и особенностей работы телевизионных радиосистем; – изучение принципов построения отдельных устройств радиотехнических систем приема и передачи информации. <p>2. Место дисциплины в структуре образовательной программы подготовки специалиста</p> <p>Дисциплина входит в вариативную часть образовательного стандарта.</p> <p>Для изучения дисциплины необходимы знания (умения, владения) сформированные в результате изучения дисциплин:</p> <ul style="list-style-type: none"> «Физика», «Математический анализ», «Информатика», «Электроника и схемотехника». <p>Дисциплина является необходимой в изучении последующих дисциплин:</p> <ul style="list-style-type: none"> «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем». <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины «Основы радиотехники» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать</p> <ul style="list-style-type: none"> – 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. <p>Уметь:</p> <ul style="list-style-type: none"> – 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>узлов систем передачи информации.</p> <p>Владеть:</p> <ul style="list-style-type: none"> – 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. <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> – 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. <p>Уметь:</p> <ul style="list-style-type: none"> – 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. <p>Владеть:</p> <ul style="list-style-type: none"> – 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 <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Основы построения радиотехнических устройств приема и передачи информации</p> <ol style="list-style-type: none"> 1.1. Основные понятия, термины и определения 1.2. Классификация и структура построения радиотехнических систем связи и вещания. 1.3. Диапазоны частот и сигналы. 1.4. Особенности распространения радиоволн различных 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>диапазонов.</p> <p>1.5. Построение радиотехнических систем.</p> <p>1.6. Антенно-фидерные устройства.</p> <p>1.7. Радиоприемные устройства.</p> <p>1.8. Радиопередающие устройства.</p> <p>2. Преобразование информационных сигналов в радиотехнических системах и коммуникационных сетях</p> <p>2.1. Сигналы, передаваемые в системах радиосвязи и телевидения.</p> <p>2.2. Виды представления сигналов.</p> <p>2.3. Спектры периодических колебаний</p> <p>2.4. Спектры непериодических колебаний.</p> <p>2.6. Виды сообщений и их характеристики. Информация, сообщения, сигналы.</p> <p>2.7. Принцип передачи информации. Виды сигналов</p> <p>2.8. Принципы преобразования аналоговых сообщений</p> <p>2.9. Международные стандарты аналого-цифрового преобразования и сжатия аудио и визуальной информации.</p> <p>3. Радиотехнические способы защиты информации</p> <p>3.1. Телекоммуникационные системы электросвязи</p> <p>3.2. Архитектура и принципы построения сетей</p> <p>3.3. Каналы связей и их математические модели</p> <p>3.4. Многоканальные телекоммуникационные системы</p> <p>3.5. Цифровые телекоммуникационные сети</p> <p>3.6. Распределение информации в телекоммуникационных сетях</p> <p>3.7. Интеграция и конвергенция цифровых телекоммуникационных сетей</p>	
<p>Б1.В.ДВ.0 1.02</p>	<p>Физические основы передачи информации</p> <p>1. Цели освоения дисциплины</p> <p>Целью освоения дисциплины «Физические основы передачи информации» является формирование способности анализировать физические явления и процессы, в системах передачи информации по проводным, беспроводным и волоконно-оптическим линиям связи, применять соответствующий математический аппарат в этой области, применять знания электроники и схемотехники при разработке защищенных компонентов автоматизированных систем.</p> <p>Эта цель достигается в ходе выполнения следующих задач:</p> <ul style="list-style-type: none"> – изучение физических сред передачи данных, типов линий связи и их характеристик; – изучение основ излучения, распространения и приема радиоволн; – изучение методов формирования и преобразования сигналов; – изучение принципов построения систем передачи информации; 	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i> 180 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>– изучение структурных схем и особенностей работы систем многоканальной связи;</p> <p>– изучение принципов построения отдельных устройств систем приема и передачи информации.</p> <p>2. Место дисциплины в структуре образовательной программы подготовки специалиста</p> <p>Дисциплина входит в вариативную часть образовательного стандарта.</p> <p>Для изучения дисциплины необходимы знания (умения, владения) сформированные в результате изучения дисциплин:</p> <p>«Физика», «Математический анализ», «Информатика», «Электроника и схемотехника».</p> <p>Дисциплина является необходимой в изучении последующих дисциплин:</p> <p>«Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем».</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины «Основы радиотехники» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать</p> <ul style="list-style-type: none"> – 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. <p>Уметь:</p> <ul style="list-style-type: none"> – 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. <p>Владеть:</p> <ul style="list-style-type: none"> – математическим аппаратом для описания процессов, 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>происходящих в системах передачи информации в целом;</p> <ul style="list-style-type: none"> – математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации; – математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации. <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> – 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. <p>Уметь:</p> <ul style="list-style-type: none"> – создавать имитационные модели 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. <p>Владеть:</p> <ul style="list-style-type: none"> – 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 <p>Дисциплина включает в себя следующие разделы:</p> <p>Системы связи и способы передачи информации</p> <ol style="list-style-type: none"> 1.1. Сообщения и сигналы. 1.2. Системы связи. Канал связи. Помехи и искажения в канале. 1.3. Кодирование и модуляция. Демодуляция и декодирование. 1.4. Дискретизация и кодирование непрерывных сообщений. 1.5. Основные характеристики систем связи. <p>2. Сообщения, сигналы, помехи</p> <ol style="list-style-type: none"> 2.1. Сообщения, сигналы и помехи как случайные процессы. Спектры случайных процессов. 2.2. Математические способы представления сигналов. 2.3. Теорема Котельникова. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>2.4. Информационные параметры сообщений и сигналов</p> <p>3. Каналы связи и их характеристики</p> <p>3.1. Общие сведения о каналах связи.</p> <p>3.2. Прохождение сигналов через каналы с детерминированными характеристиками.</p> <p>3.3. Математические модели каналов связи.</p> <p>3.4. Пропускная способность канала связи.</p> <p>3.5. Теорема кодирования для канала с помехами.</p> <p>4. Передача дискретных сообщений в непрерывных каналах</p> <p>4.1. Прием сигнала как статистическая задача. Критерии качества приема дискретных сообщений.</p> <p>4.2. Оптимальные алгоритмы приема при полностью известных сигналах и при сигналах с неопределенной фазой.</p> <p>5. Основы теории кодирования</p> <p>5.1. Назначение и классификация кодов. Принципы помехоустойчивого кодирования</p> <p>5.2. Линейные двоичные блочные коды. Разновидности систематических кодов</p> <p>5.3. Эквивалентная вероятность ошибки. Системы с обратной связью.</p> <p>6. Теория передачи непрерывных сообщений</p> <p>6.1. Источник непрерывных сообщений и его производительность. Верность передачи непрерывных сообщений.</p> <p>6.2. Оптимальный прием непрерывных сообщений.</p> <p>6.3. Помехоустойчивость систем аналоговой передачи при слабых помехах. Порог помехоустойчивости. Помехоустойчивость систем с импульсной модуляцией.</p> <p>6. Цифровые методы передачи непрерывных сообщений</p> <p>6.1. Общие сведения о цифровой передаче непрерывных сообщений.</p> <p>6.2. Помехоустойчивость импульсно-кодовой модуляции. Кодирование с предсказанием.</p> <p>6.3. Эффективность систем связи.</p> <p>7. Теория многоканальной передачи сообщений</p> <p>7.1. Основы теории разделения сигналов.</p> <p>7.2. Частотное, временное и фазовое разделение сигналов. Разделение сигналов по форме.</p> <p>7.3. Способы разделения сигналов в асинхронных адресных системах связи</p>	
Б1.В.ДВ.02	Дисциплины по выбору Б1.В.ДВ.02	
Б1.В.ДВ.02.01	<p>Основы теории оптимизации</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью дисциплины «Основы теории оптимизации» является</p>	Общая трудоемкость

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>освоение студентами базовых понятий теории методов оптимизации, формирование представлений об алгоритмах решения задач и их использовании для решения прикладных задач в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Основы теории оптимизации входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Дискретная математика Математический анализ Теория вероятностей, математическая статистика Алгебра и геометрия Теория информации Языки программирования Информатика Математическая логика и теория алгоритмов Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Разработка и эксплуатация защищенных автоматизированных систем Криптографические методы защиты информации Тестирование систем защиты информации автоматизированных систем Алгоритмы шифрования информации Моделирование угроз информационной безопасности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения</p> <p>дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Основы теории оптимизации» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> — Общие положения теории оптимизации; — Логическую, функциональную и структурную схему 	<p><i>дисциплины составляет 4 зачетных единицы</i> 144 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>персонального компьютера, устройства организующие работу вычислительных систем;</p> <ul style="list-style-type: none"> — Способы применения теоретических положений и методов теории оптимизации для постановки и решения профессиональных задач. <p>Уметь</p> <ul style="list-style-type: none"> — 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 <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>ПК-2 способностью создавать и исследовать модели автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные информационные технологии, используемые в автоматизированных системах; — Классификацию современных автоматизированных систем; — Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем. <p>Уметь</p> <ul style="list-style-type: none"> — 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; — Находить оптимальные стратегии. <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные понятия математического анализа, дифференциальной геометрии, численные методы оптимизации <p>Уметь</p> <ul style="list-style-type: none"> — 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 <p>Владеть</p> <ul style="list-style-type: none"> — Основными методами оптимизации; — Методами оптимизации средствами вычислительной техники; — Навыками реализации задач оптимизации посредством программного обеспечения общего назначения и методо-ориентированного программного обеспечения <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Предмет и содержание дисциплины <ol style="list-style-type: none"> 1.1 Введение в теорию оптимизации. Предмет и задачи исследования теории оптимизации. 1.2 Основные положения теории оптимизации. Основные термины и понятия. 2. Линейное программирование. Методы решения ЗЛП <ol style="list-style-type: none"> 2.1 Основные положения линейного программирования. Основные термины и понятия. 2.2 Методы решения задач линейного программирования. Графический метод. Симплексный метод. 3. Применение общей задачи линейного программирования для решения прикладных <ol style="list-style-type: none"> 3.1 Закрытая модель транспортной задачи. Открытая модель транспортной задачи. Постановка задачи и ее математическая модель. Программная реализация открытой и закрытой ТЗ. 3.2 Транспортная задача с дополнительными ограничениями. Приложения транспортной задачи для решения задач из различных предметных областей. Программная реализация задач 3.3 Построение математической модели для решения сетевых задач. Решение сетевых задач методами линейного программирования. Программная реализация задач 3.4 Решение сетевой задачи о максимальном потоке. Решение задачи о кратчайшем пути. 4. Решение задач комбинаторной оптимизации <ol style="list-style-type: none"> 4.1 Решение задачи о рюкзаке. Постановка задачи и ее 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>математическая модель. Программная реализация задачи.</p> <p>4.2 Применение задачи об укладке рюкзака к алгоритмам шифрования. Программная реализация задачи.</p> <p>5. Моделирование систем. Решение задач одномерной оптимизации</p> <p>5.1 Решение задач одномерной оптимизации. Методом перебора значений функции. Метод Ньютона и его модификации. Постановка задачи и ее математическая модель.</p> <p>5.2 Решение задач одномерной оптимизации методом золотого сечения. Постановка задачи и ее математическая модель. Программная реализация задачи.</p> <p>6. Моделирование систем. Решение задач многомерной оптимизации</p> <p>6.1 Решение задач многомерной оптимизации методом покоординатного спуска. Постановка задачи и ее математическая модель. Программная реализация</p> <p>6.2 Решение задач многомерной оптимизации градиентными методами. Постановка задачи и ее математическая модель. Программная реализация</p> <p>6.3 Использование генетических алгоритмов для решения задач многомерной оптимизации. Постановка задачи и ее математическая модель. Программная реализация задачи.</p> <p>7. Решение прикладных задач методами оптимизации</p> <p>7.1 Примеры решения прикладных задач методами оптимизации. Постановка задачи и ее математическая модель. Программная реализация задачи.</p>	
Б1.В.ДВ.0 2.02	<p>Математическое моделирование распределенных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями изучения дисциплины «Математическое моделирование распределенных систем» являются: освоение моделей управления, получение знаний о закономерностях и свойствах процессов управления распределенными объектами, систематическое изучение основ теории и практики математического и имитационного моделирования систем; изучение основных подходов и математических схем к построению имитационных моделей; изучение возможностей применения имитационных моделей; освоение методологий и актуальных CASE-средств для имитационного моделирования систем и процессов и формировании у обучающихся навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Математическое моделирование распределенных</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i></p> <p>144</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>систем входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Алгебра и геометрия Математический анализ Математическая логика и теория алгоритмов Теория вероятностей, математическая статистика</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Моделирование систем и процессов защиты информации Моделирование угроз информационной безопасности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Математическое моделирование распределенных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ОПК-2 способностью 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</p> <p>Знать</p> <ul style="list-style-type: none"> — 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. <p>Уметь</p> <ul style="list-style-type: none"> — применять математические методы для анализа общих свойств линейных распределенных систем; — применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами; — применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований. <p>Владеть</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— методами преобразования структурных схем распределенных систем управления;</p> <p>— методами преобразования структурных схем распределенных систем управления;</p> <p>— методами и навыками преобразования структурных схем распределенных систем управления.</p> <p>ПК-2 способностью создавать и исследовать модели автоматизированных систем</p> <p>Знать</p> <p>— Принципы и методы проектирования программно-аппаратного обеспечения;</p> <p>— Принципы и методы проектирования программно-аппаратного обеспечения;</p> <p>— Методы планирования и организации работ по защите информации.</p> <p>Уметь</p> <p>— Разрабатывать и использовать профили защиты и задания по безопасности;</p> <p>— Готовить проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;</p> <p>— Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы.</p> <p>Владеть</p> <p>— Навыками разработки технических заданий, рабочих проектов, планов и графиков проведения работ по защите информации;</p> <p>— Навыками выполнения требований нормативно-технической документации по соблюдению установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации;</p> <p>— Навыками проектирования программных и аппаратных средств защиты информации в соответствии с техническим заданием.</p> <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <p>— Основные принципы и схемы автоматического управления;</p> <p>— Основные требования нормативно-правовой базы в области защиты информации;</p> <p>— Основные уязвимости защищенных компьютерных систем;</p> <p>— Модели безопасности компьютерных систем;</p> <p>— Методы проведения расследования компьютерных преступлений,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>правонарушений и инцидентов;</p> <ul style="list-style-type: none"> — Математические методы для анализа общих свойств распределенных систем. <p>Уметь</p> <ul style="list-style-type: none"> — 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 <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>Дисциплина включает в себя следующие разделы</p> <ol style="list-style-type: none"> 1. Математическое моделирование <ol style="list-style-type: none"> 1.1 Форма и принципы представления математических моделей. Моделирование как метод научного исследования. Типы моделей 1.2 Моделирование динамических характеристик систем с сосредоточенными параметрами 2. Особенности построения математических моделей <ol style="list-style-type: none"> 2.1 Подходы к построению моделей сложных систем. 2.2 Имитационное моделирование случайных процессов в измерительных приборах и системах. 2.3 Математические модели в интегральной форме. 2.4 Уравнения Лапласа и Пуассона. Физическая интерпретация 3 типов граничных условий. Сеточные модели и их реализация 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>численными методами теории цепей</p> <p>2.5 Решение краевых задач методами конечно - разностной аппроксимации по координатам в системах математического моделирования для персональных компьютеров. Условия устойчивости решений. Особенности моделирования физических полей в неоднородных и анизотропных средах.</p> <p>3. Компьютерное моделирование и вычислительный эксперимент</p> <p>3.1 Понятие псевдослучайности. Псевдослучайные объекты.</p> <p>3.2 Базовый датчик: критерии качества, используемые методы. Генерация непрерывных случайных величин: метод отбраковки и метод обратной функции.</p> <p>3.3 Специальные методы генерации нормально распределённых случайных величин</p> <p>3.4 Генерация дискретных случайных величин, выборка с возвращением и выборка без возвращения.</p> <p>3.5 Генерация случайных процессов: основные подходы. Генерация Гауссовских процессов. Решение математических моделей</p> <p>4. Компьютерное имитационное моделирование</p> <p>4.1 Статистическое имитационное моделирование</p> <p>4.2 Особенности имитационного моделирования. Этапы имитационного моделирования.</p> <p>5. Статистическое имитационное моделирование</p> <p>5.1 Математическое моделирование стационарных физических полей в системах с распределенными параметрами.</p> <p>5.2 Математическое моделирование нестационарных полей в системах с распределенными параметрами.</p> <p>:</p>	
Б1.В.ДВ.03	Дисциплины по выбору Б1.В.ДВ.03	
Б1.В.ДВ.03.01	<p>Защита электронного документооборота</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью изучения дисциплины «Защита электронного документооборота» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой информации в системах электронного документооборота, анализом возможных угроз в информационной сфере и адекватных мер по их нейтрализации, совершенствование практических навыков по организации защиты информации в организациях, в том числе на предприятии и в учреждениях.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Защита электронного документооборота входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i></p> <p>144</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>практик:</p> <p>Криптографические методы защиты информации Моделирование угроз информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Разработка эксплуатационной документации на системы защиты информации автоматизированных систем Безопасность операционных систем Информационная безопасность распределенных информационных систем Методы выявления нарушений информационной безопасности, аттестация АИС Организационное и правовое обеспечение информационной безопасности Тестирование систем защиты информации автоматизированных систем Техническая защита информации Безопасность сетей ЭВМ Безопасность систем баз данных Математическое моделирование распределенных систем Основы теории оптимизации Программно-аппаратные средства обеспечения информационной безопасности Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Защита электронного документооборота» обучающийся должен обладать следующими компетенциями: ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> - основные понятия предметной области систем электронного документооборота -основные информационные технологии, используемые в 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>автоматизированных системах; – принципы построения и функционирования, примеры реализаций систем электронного документооборота; нормативные правовые акты в области защиты информации</p> <p>Уметь</p> <ul style="list-style-type: none"> -применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем электронного документооборота - моделировать потоки информации и документов, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности -готовить научно-технические отчеты, обзоры, публикации по теме предметной области <p>Владеть</p> <ul style="list-style-type: none"> -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 <p>ПК-28 способностью управлять информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> -нормативные акты, используемые при разработке политики информационной безопасностью организации; – основные критерии оценки защищенности систем электронного документооборота, источники угроз <p>методические рекомендации отраслевых регуляторов по обеспечению информационной безопасности</p> <p>Уметь</p> <ul style="list-style-type: none"> - 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 <p>Владеть</p> <ul style="list-style-type: none"> - 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; <p>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>организациях, в том числе на предприятии и в учреждении</p> <p>Знать</p> <p>– принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности</p> <p>Уметь</p> <p>-выявлять особенности и формировать требования к системе организации коллективной работы с информационными ресурсами СЭД</p> <p>-формировать комплекс мер по защите информации с учетом соответствия нормативным документам, технической реализуемости и экономической целесообразности;</p> <p>Владеть</p> <p>-навыками администрирования систем электронного документооборота</p> <p>-навыками настройки систем предотвращения утечек информации</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Функции, задачи и особенности электронного документооборота</p> <p>1.1 Основные понятия и принципы электронного документооборота. Теоретические и организационные основы создания систем электронного документооборота организации.</p> <p>1.2 Методологические основы разработки информационной системы электронного документооборота. Классификация систем электронного документооборота. Государственные услуги, банковское обслуживание, электронные закупки.</p> <p>1.3 Применение нормативно-правовых актов по защите информации в СЭДО. ГОСТ Р 53898-2010</p> <p>1. Угрозы безопасности для систем электронного документооборота</p> <p>2.2 Угрозы целостности и доступности СЭДО. Угроза доступа сервера ОС. Угроза сервера СЭД. Контроль целостности электронного документа.</p> <p>2.1 Угроза конфиденциальности. Угроза доступа рабочих мест. Угроза доступа сервера ОС. Угроза сервера СЭД. Угроза перехвата каналов связи</p> <p>3. Проблемы применения ЭЦП в системах электронного документооборота</p> <p>3.1 Проблемы подлинности документов в системе ЭДО.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Применение Электронно-цифровой подписи в соответствии с уровнем юридической значимости документа.</p> <p>3.2 Регламент использования электронных средств обмена документами в зависимости от уровня взаимодействия(внутри организации, межорганизационный, межведомственный)</p> <p>3.3 Проблемы «отчуждения» ключей электронной подписи и возможные способы их решения</p> <p>4. Проблемы аутентификации пользователей систем электронного документооборота</p> <p>4.1 Разграничение прав доступа к объектам. Ограничение доступа на интерфейсном уровне.</p> <p>5. Использование DLP – систем для предотвращения утечек СЭД</p> <p>5.1 Обзор и сравнение российских и зарубежных dlp-систем.</p> <p>5.2 Идентификация и профайлинг пользователей пользователей. Создание правил безопасности.</p> <p>5.3 Фильтрация трафика при перехвате. Организация защищенной системы электронной почты. Цифровые отпечатки</p> <p>5.4 Оценка эффективности защиты СЭД. Оценка по экономической эффективности. Методы оценки по интегральному эффекту («линейная свертка» частных показателей, методы теории нечетких множеств).</p> <p>6. Аппаратная защита технологии электронного обмена информацией</p> <p>6.1 Применение аппаратных средств защиты информации в системах электронного документооборота.</p> <p>7. Проектирование и внедрение защищенного электронного документооборота</p> <p>7.1 Проектирование организационных, программных, аппаратных и иных средств СЗИ. Особенности эксплуатации защищенных систем электронного документооборота.</p> <p>7.2 Анализ эффективности и разработка мер по совершенствованию СЗИ СЭД.</p>	
Б1.В.ДВ.0 3.02	<p>Информационная безопасность систем организационного управления</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целью изучения дисциплины «Информационная безопасность систем организационного управления» является теоретическая и практическая подготовка к деятельности, связанной с защитой информации в автоматизированных системах организационного управления, анализом возможных угроз в информационной сфере и адекватных мер по их нейтрализации, совершенствование практических навыков по организации защиты информации в организациях, в том числе на предприятии и в</p>	<p><i>Общая трудоемкость дисциплины составляет 4 зачетных единицы</i> 144</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>учреждениях.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Информационная безопасность систем организационного управления входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Криптографические методы защиты информации Моделирование угроз информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Разработка эксплуатационной документации на системы защиты информации автоматизированных систем Безопасность операционных систем Информационная безопасность распределенных информационных систем Методы выявления нарушений информационной безопасности, аттестация АИС Организационное и правовое обеспечение информационной безопасности Тестирование систем защиты информации автоматизированных систем Техническая защита информации Безопасность сетей ЭВМ Безопасность систем баз данных Математическое моделирование распределенных систем Основы теории оптимизации Программно-аппаратные средства обеспечения информационной безопасности</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Информационная безопасность систем организационного управления» обучающийся должен обладать следующими</p>	<p>акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>компетенциями:</p> <p>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> -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 <p>Уметь</p> <ul style="list-style-type: none"> -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 <p>Владеть</p> <ul style="list-style-type: none"> -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 <p>ПК-28 способностью управлять информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> -методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью <p>Уметь</p> <ul style="list-style-type: none"> -разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-готовить предложения для актуализации организационных мер по защите информационных систем ОУ</p> <p>Владеть</p> <ul style="list-style-type: none"> -терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации <p>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении</p> <p>Знать</p> <ul style="list-style-type: none"> - основные понятия организации обеспечения информационной безопасности -основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности <p>Уметь</p> <ul style="list-style-type: none"> -анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны при выполнении функциональных обязанностей; - организовывать и обеспечивать сохранение режима конфиденциальности при выполнении функциональных обязанностей; <p>Владеть</p> <ul style="list-style-type: none"> -методами формирования требований по защите объекта; -методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Классификация систем ОУ</p> <p>1.1. Классификация систем ОУ по функциям управления; по видам управляющих команд; по степени сосредоточения власти</p> <p>1.2. Технологическое обеспечение, информационные процессы в автоматизированных системах организационного управления.</p> <p>1.3. Концепции создания и развития объекта управления и системы организационного управления</p> <p>2 Угрозы систем организационного управления</p> <p>2.1 Анализ источников угроз и проектирование модели разграничения прав доступа для АИС ОУ</p> <p>3.Управление правами доступа</p> <p>3.1 Разграничение прав доступа к объектам. Ограничение доступа на интерфейсном уровне.</p> <p>3.2 Задание доступа на уровне серверной базы данных.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>3.3 Идентификация и профайлинг пользователей. 3.5 Применение аппаратных средств защиты информации в АИС организационного управления 4. Организация реагирования на чрезвычайные ситуации (инциденты) 8.1 Экзамен</p>	
Б1.В.ДВ.04	Дисциплины по выбору Б1.В.ДВ.04	
Б1.В.ДВ.04.01	<p>Виртуальные сети 1 Цели освоения дисциплины (модуля) Целями освоения дисциплины «Виртуальные сети» являются овладение студентами необходимым и достаточным уровнем профессиональных, профессионально-специализированных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Виртуальные сети» являются: - изучение архитектуры и настроек виртуальных локальных сетей (VLAN); - изучение структуры, принципов работы, настроек виртуальных частных сети (VPN) и технологий на их основе Site-to-site VPN, FlexVPN и SSL VPN; - освоение облачных технологий виртуальных сетей. 2 Место дисциплины (модуля) в структуре образовательной программы Дисциплина Виртуальные сети входит в вариативную часть учебного плана образовательной программы. Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик: Информатика Организация ЭВМ и вычислительных систем Сети и системы передачи информации Безопасность сетей ЭВМ Безопасность операционных систем Разработка и эксплуатация защищенных автоматизированных систем Управление информационной безопасностью Моделирование угроз информационной безопасности Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Защита электронного документооборота Информационная безопасность систем организационного управления Методы проектирования защищенных распределенных</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единицы 180 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационных систем Производственная-преддипломная практика Научно-исследовательская работа 3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Виртуальные сети» обучающийся должен обладать следующими компетенциями: 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</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 сетей в облачных сетевых структурах. <p>Уметь</p> <ul style="list-style-type: none"> - Создавать защищенные вычислительные сети с применением виртуализации; - Применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях. <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> - Информационно-технологические ресурсы автоматизированных систем; - Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности. <p>Уметь</p> <ul style="list-style-type: none"> - Создавать виртуальные сети для обеспечения эффективного применения информационно-технологических ресурсов 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>автоматизированной системы с учетом требований информационной безопасности;</p> <ul style="list-style-type: none"> -Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности. <p>Владеть</p> <ul style="list-style-type: none"> -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. <p>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> -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. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению информационной безопасности.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Виртуальные локальные сети (VLAN).</p> <p>1.1 Типы VLAN, сегментация VLAN. голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet.</p> <p>1.2 Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Поиск неисправностей при использовании VLAN.</p> <p>1.3 Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.</p> <p>2. Виртуальные частные сети (VPN). Сетевые технологии Site-to-site VPN, FlexVPN и SSL VPN. Настройка и использование Cisco AnyConnect VPN.</p> <p>2.1 Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Основные компоненты VPN-технологии.</p> <p>2.2 Протоколы работы VPN: GRE, PPTP, L2TP, PPPoE. Конфигурирование соединения</p> <p>2.3 Протокол ISAKMP. Технология IPsec, Совместная работа IPSEC и NAT. Транзитная передача зашифрованного трафика.</p> <p>2.4 Dynamic VPN, конфигурирование функций динамического VPN-концентратора. Конфигурирование сервиса DynDNS.</p> <p>2.5 Конфигурирование классического туннельного соединения для объединения офисных сетей. Развёртывание DMVPN на устройствах с Cisco IOS. IPsec VPN с использованием SDM.</p> <p>2.6 Технология FlexVPN. Основные преимущества и возможности технологии FlexVPN.. Централизованное конфигурирование узлов-участников.</p> <p>2.7 Технология SSL VPN. Групповые политики SSL-клиентов на Cisco ASA и connection profiles. Настройка SSL VPN на Cisco ASA. Аутентификация через внешний AAA-сервер и использование локального/внешнего CA</p> <p>2.8 Настройка и использование Cisco AnyConnect VPN. Мониторинг работы AnyConnect VPN. Настройка специфических аспектов работы AnyConnect VPN.</p> <p>3. Облачные технологии виртуальных сетей.</p> <p>3.1 Характеристики аппаратно-программных платформ виртуализации для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS</p> <p>3.2 Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>3.3 Реализации служб DNS, WINS, DHCP, NAT в виртуальной сетевой среде. Создание виртуальных Web-серверов в облаке, балансировка сетевой нагрузки в облаке для веб-серверов (NLB).</p> <p>3.4 Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA).</p> <p>3.5 Создание VPN-серверов для виртуальных частных сетей в облаке.</p> <p>3.6 Облачная среда передачи данных Data Center Bridging (DCB), расширенный протокол xSTP, метод передачи трафика сети хранения данных Fibre Channel по сети Ethernet. FCoE технология</p>	
<p>Б1.В.ДВ.0 4.02</p>	<p>Защита программного обеспечения</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями изучения дисциплины «Защита программного обеспечения» являются: освоение технических средств защиты, нормативно-правовых документов и организационных методов в области обеспечения защиты от несанкционированного использования и копирования программного обеспечения; методов противодействия разрушению, нарушения целостности и достоверности программного обеспечения; частных политик информационной безопасности автоматизированной системы в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Защита программного обеспечения входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Безопасность операционных систем Техническая защита информации Разработка и эксплуатация защищенных автоматизированных систем Технология построения защищенных распределенных приложений Технологии и методы программирования Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных единиц</i> 180 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>В результате освоения дисциплины (модуля) «Защита программного обеспечения» обучающийся должен обладать следующими компетенциями:</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. <p>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> — способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ; — Нормативные документы по стандартизации и сертификации 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>программной защиты.</p> <ul style="list-style-type: none"> — Цели и задачи разработки политики информационной безопасности — Методы и средства анализа достаточности мер по обеспечению ИБ ПО <p>Уметь</p> <ul style="list-style-type: none"> — Разрабатывать порядок эксплуатации программного обеспечения — Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения — Проводить мониторинг и аудит защищенности ПО <p>Владеть</p> <ul style="list-style-type: none"> — Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО — Методами контроля соблюдения политики учетных записей <ul style="list-style-type: none"> — Навыками регламентации обслуживания и осуществления модификации программного обеспечения <p>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - разрабатывать и администрировать базы данных в соответствии с требованиями информационной безопасности; - настраивать защиту программного обеспечения с применением дистанционного администрирования <p>Владеть</p> <ul style="list-style-type: none"> - методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств; - в полной мере средствами администрирования БД в интегрированных средах СУБД. <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Введение в теорию обеспечения безопасности программного обеспечения и данных</p> <p>1.1 Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.</p> <p>1.2 Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.3 Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.</p> <p>2. Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность</p> <p>2.1 Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.</p> <p>2.2 Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.</p> <p>3. Методы и средства обеспечения целостности и достоверности используемого программного кода</p> <p>3.1 Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.</p> <p>3.2 Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу.</p> <p>3.3 Основные подходы к защите программного обеспечения от несанкционированного копирования.</p> <p>4. Администрирование и защита БД</p> <p>4.1 Понятия администрирование, привилегия, доступ. Виды пользователей и группы привилегий, соответствующие виду пользователя.</p> <p>4.2 Программные и программно-аппаратные средства защиты БД</p> <p>4.3 Контроль доступа к данным. Управление привилегиями пользователей базы данных. Идентификация и аутентификация пользователя. Пароли.</p> <p>4.4 Транзакционный подход к организации доступа к данным. Понятие SQL Injection. Виды уязвимостей, используемые атаками SQL Injection. Методы защиты от Injection.</p> <p>4.5 Использование аудита БД. Аудит системных событий. Системы обнаружения вторжений.</p> <p>5. Экзамен</p>	
Б1.В.ДВ.05	Дисциплины по выбору Б1.В.ДВ.05	
Б1.В.ДВ.05.01	<p>Методы мониторинга информационной безопасности автоматизированных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Общей целью дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в</p>	<p><i>Общая трудоемкость дисциплины составляет 5 зачетных</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Специальными целями дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» являются: изучить архитектуру, функции, методы и алгоритмы, организационную структуру, технологии создания и готовые аппаратно-программные решения систем мониторинга информационной безопасности автоматизированных систем; научиться применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем; выполнять аудит информационной безопасности информационных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Методы мониторинга информационной безопасности АС входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Информатика Организация ЭВМ и вычислительных систем Техническая защита информации Моделирование систем и процессов защиты информации Организационное и правовое обеспечение информационной безопасности Безопасность сетей ЭВМ Моделирование угроз информационной безопасности Управление информационной безопасностью Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Методы мониторинга информационной безопасности АС» обучающийся должен обладать следующими компетенциями: ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты</p>	<p><i>единицы</i> 180 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> - способы организации автоматизированных систем; - подходы к проведению сертификации средств защиты информационной безопасности; <p>Уметь</p> <ul style="list-style-type: none"> - составлять регламент испытаний средств защиты информации автоматизированных систем; <p>Владеть</p> <ul style="list-style-type: none"> - навыками применения, специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем; <p>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>Знать</p> <ul style="list-style-type: none"> - перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации; <p>Уметь</p> <ul style="list-style-type: none"> - применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов; <p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе; <p>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> - методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы; <p>Уметь</p> <ul style="list-style-type: none"> - выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности; <p>Владеть</p> <ul style="list-style-type: none"> - навыками определения возможных векторов атаки на автоматизированную систему; <p>ПСК-7.3 способностью проводить аудит защищенности</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационно- технологических ресурсов распределенных информационных систем</p> <p>Знать</p> <ul style="list-style-type: none"> - способы получения информации о внутренней структуре исследуемой распределенной системе; -наиболее распространённые точки для несанкционированного входа в распределенную систему; <p>Уметь</p> <ul style="list-style-type: none"> - проводить анализ уязвимостей распределённой системы; - получать несанкционированный доступ к ресурсам распределенной системы; <p>Владеть</p> <ul style="list-style-type: none"> - навыками противодействия внешним атакам на распределенную информационную сеть; <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Введение в мониторинг АС <ol style="list-style-type: none"> 1.1 Архитектура и функции систем мониторинга информационной безопасности. 1.2 Модульный принцип построения системы информационной безопасности. 2. Мониторинг ИБ АС <ol style="list-style-type: none"> 2.1 Идентификация пользователей, трафика, приложений, протоколов и схем использования ресурсов. 2.2 Ограничение доступа и использования ресурсов на уровне пользователя, протокола, сервиса и приложения. Изоляция пользователей, сервисов и приложений 3. Средства мониторинга ИБ АС <ol style="list-style-type: none"> 3.1 Применение специализированных дистрибутивов Linux для создания АРМ системы мониторинга ИБ АС 3.2 Установка и настройка дистрибутива Kali Linux 2 4. Аудит проводных сетей <ol style="list-style-type: none"> 4.1 Способы организации зеркалирования трафика. 4.2 Способы обнаружения угроз по сетевой активности 5. Аудит беспроводных сетей <ol style="list-style-type: none"> 5.1 Получение доступа к беспроводной сети 5.2 Способы противодействия атакам на беспроводную сеть 6. Аудит Web-ресурсов <ol style="list-style-type: none"> 6.1 Аудит средств авторизации 6.2 Защита от SQL инъекций 	
Б1.В.ДВ.0 5.02	<p>Анализ безопасности программного обеспечения</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Общей целью дисциплины «Анализ безопасности программного обеспечения» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей</p>	<i>Общая трудоемкость дисциплины</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ступени образования, и овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Анализ безопасности программного обеспечения» являются:</p> <ul style="list-style-type: none"> - изучить контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения и способы обеспечения надежности программ для контроля их технологической безопасности; - освоить способы оценки эффективности систем защиты программного обеспечения и технологии разработки систем программно-технической защиты программного обеспечения. <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Анализ безопасности программного обеспечения входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Виртуальные сети Защита программного обеспечения Защита электронного документооборота Методы мониторинга информационной безопасности АС Информационная безопасность систем организационного управления Организация ЭВМ и вычислительных систем Информатика Языки программирования Основы информационной безопасности Технологии и методы программирования Технология построения защищенных распределенных приложений Информационные технологии. Базы данных Безопасность сетей ЭВМ Безопасность систем баз данных Тестирование систем защиты информации автоматизированных систем</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Научно-исследовательская работа Подготовка к защите и защита выпускной квалификационной работы Подготовка к сдаче и сдача государственного экзамена Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате</p>	<p><i>составляет 5 зачетных единиц 180 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>освоения дисциплины (модуля) и планируемые результаты обучения В результате освоения дисциплины (модуля) «Анализ безопасности программного обеспечения» обучающийся должен обладать следующими компетенциями: ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем Знать - Нормативные документы по метрологии, стандартизации и сертификации программных средств защиты; - подходы к проведению сертификации информационной безопасности программного обеспечения; Уметь - составлять регламент испытаний информационной безопасности программного обеспечения; Владеть - навыками применения, специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем; ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации Знать - перечень инструментов для проведения анализа безопасности программного обеспечения; - базовый функционал инструментов для проведения анализа безопасности программного обеспечения; Уметь - применять технические средства для проведения анализа безопасности программного обеспечения; Владеть - навыками работы с специализированным программным обеспечением для проведения анализа безопасности программного обеспечения ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности Знать - методы повышения уровня безопасности программного обеспечения; Уметь - выполнять работы по оптимизации схем управления автоматизированной системой; - выявлять компоненты программного обеспечения, не</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обеспечивающие требуемый уровень информационной безопасности;</p> <p>Владеть</p> <ul style="list-style-type: none"> - навыками определения возможных векторов атаки на программное обеспечение; <p>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем</p> <p>Знать</p> <ul style="list-style-type: none"> - Способы обработки исключительных ситуаций; - Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения. <p>Уметь</p> <ul style="list-style-type: none"> - проводить анализ уязвимостей программного обеспечения; - выполнять реверс инжиниринг программного обеспечения; <p>Владеть</p> <ul style="list-style-type: none"> - навыками противодействия атакам на программное обеспечение; <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Теоретические и формальные методы доказательства правильности программ и их спецификаций <ol style="list-style-type: none"> 1.1 Языки формальной спецификации программ. Валидация сценариев требований 1.2 Методы анализа структур программ. Верификация и валидация программ. Метод верификации композиции правильных компонентов 2. Контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения <ol style="list-style-type: none"> 2.1 Проблемы анализа безопасности программного обеспечения. Основные угрозы безопасности программного обеспечения. 2.2 Алгоритмические и программные закладки 3. Методы и средства анализа безопасности программ <ol style="list-style-type: none"> 3.1 Лексический и синтаксический верификационный анализ, семантический анализ программ. Верификация моделей программ методом model checking. 3.2 Логика дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации 4. Способы обеспечения надежности программ для контроля их технологической безопасности <ol style="list-style-type: none"> 4.1 Процессы обеспечения функциональной безопасности программных продуктов в стандартах IEC 61508:1-6: 1998-2000, ISO 15408:1999 93, ISO 13335: 1-5: 1998. 4.2 Методы идентификации программ и их характеристик. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов. 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>5. Анализ средств и этапы преодоления систем защиты программного обеспечения</p> <p>5.1 Методы защиты программ от исследования</p> <p>5.2 Технологии разработки систем программно-технической защиты программного обеспечения. Этапы проектирования и разработки систем программно-технической защиты программного обеспечения.</p> <p>6. Оценка эффективности систем защиты программного обеспечения</p> <p>6.1 Критерии оценки: стойкость к исследованию/взлому; отказоустойчивость (надёжность).</p> <p>6.2 Критерии оценки: независимость от конкретных реализаций операционных систем; совместимость; неудобства для конечного пользователя программного обеспечения; побочные эффекты; стоимость; доброкачественность</p>	
<p>Б1.В.ДВ. 06.01</p>	<p>Элективные курсы по физической культуре и спорту</p> <p>1 Цели освоения дисциплины (модуля)</p> <ul style="list-style-type: none"> – формирование физической культуры личности будущего профессионала, востребованного на современном рынке труда; – развитие физических качеств и способностей, совершенствование функциональных возможностей организма, укрепление индивидуального здоровья; – формирование устойчивых мотивов и потребностей в бережном отношении к собственному здоровью, в занятиях физкультурно-оздоровительной и спортивно - оздоровительной деятельностью; – овладение технологиями современных оздоровительных систем физического воспитания, обогащение индивидуального опыта занятий специально-прикладными физическими упражнениями и базовыми видами спорта; – овладение системой профессионально и жизненно значимых практических умений и навыков, обеспечивающих сохранение и укрепление физического и психического здоровья; – освоение системы знаний о занятиях физической культурой, их роли и значении в формировании здорового образа жизни и социальных ориентаций; – приобретение компетентности в физкультурно-оздоровительной и спортивной деятельности, овладение навыками творческого сотрудничества в коллективных формах занятий физическими упражнениями; – сдача нормативов Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (ГТО). <p>2 Место дисциплины (модуля) в структуре образовательной программы</p>	<p><i>Общая трудоемкость дисциплины составляет 0 зачетных единиц 328 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Дисциплина Элективные курсы по физической культуре и спорту входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>«Физическая культура» в рамках общего полного среднего образования</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Элективные курсы по физической культуре и спорту» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-9 способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности</p> <p>Знать</p> <p>основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;</p> <p>формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;</p> <p>знание технических приемов и двигательных действий базовых видов спорта;</p> <p>современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;</p> <p>основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;</p> <p>технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</p> <p>Уметь</p> <p>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;</p> <p>выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>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, 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). Дисциплина включает в себя следующие разделы: 1. Введение 1.1 Физическая культура в общекультурной и профессиональной</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>подготовке обучающихся</p> <p>1.2 Основы техники безопасности при выполнении упражнений</p> <p>2. Общефизическая подготовка (комплекс ГТО)</p> <p>2.1 Подготовка к выполнению норматива в беге на 100 м (сек)</p> <p>2.2 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз))</p> <p>2.3 Подготовка к выполнению норматива в бег на 3 км (мин)</p> <p>2.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи-см))</p> <p>2.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см))</p> <p>2.6 Подготовка к выполнению норматива (Плавание на 50 м (мин))</p> <p>3. Учебные занятия по видам спорта</p> <p>3.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p> <p>Специальное медицинское отделение</p> <p>4. Общефизическая подготовка (комплекс ГТО)</p> <p>4.1 Подготовка к выполнению норматива в беге на 100 м (сек)</p> <p>4.2 Подготовка к выполнению норматива в беге на 3 км (мин)</p> <p>4.3 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз))</p> <p>4.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см))</p> <p>4.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см))</p> <p>4.6 Подготовка к выполнению норматива (Бег на лыжах на 5 км (мин))</p> <p>4.7 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м))</p> <p>4.8 Подготовка к выполнению норматива (Плавание на 50 м (мин))</p> <p>5. Учебные занятия по видам спорта</p> <p>5.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Легкая атлетика Пауэрлифтинг и гиревой спорт Специальное медицинское отделение</p> <p>6. Общефизическая подготовка (комплекс ГТО)</p> <p>6.1 Подготовка к выполнению норматива в беге на 100 м (сек)</p> <p>6.2 Подготовка к выполнению норматива в беге на 3 км (мин)</p> <p>6.3 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз))</p> <p>6.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см))</p> <p>6.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см))</p> <p>6.6 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м))</p> <p>6.7 Подготовка к выполнению норматива (Плавание на 50 м (мин))</p> <p>6.8 Подготовка к выполнению норматива (Стрельба из пневматической винтовки из положения сидя или стоя с опорой локтей о стол или стойку, дистанция – 10 м (очки) или стрельба из электронного оружия из положения сидя или стоя с опорой локтей о стол или стойку, дистанция – 10 м (очки))</p> <p>7. Учебные занятия по видам спорта</p> <p>7.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика Пауэрлифтинг и гиревой спорт Специальное медицинское отделение</p> <p>8. Общефизическая подготовка (комплекс ГТО)</p> <p>8.1 Подготовка к выполнению норматива в беге на 100 м (сек)</p> <p>8.2 Подготовка к выполнению норматива в беге на 3 км (мин)</p> <p>8.3 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз))</p> <p>8.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см))</p> <p>8.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см))</p> <p>8.7 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м))</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>8.8 Подготовка к выполнению норматива (Плавание на 50 м (мин))</p> <p>8.9 Подготовка к выполнению норматива (Стрельба из пневматической винтовки из положения сидя или стоя с опорой локтей о стол или стойку, дистанция – 10 м (очки) или стрельба из электронного оружия из положения сидя или стоя с опорой локтей о стол или стойку, дистанция – 10 м (очки))</p> <p>9. Учебные занятия по видам спорта</p> <p>9.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p> <p>Специальное медицинское отделение</p> <p>10. Учебные занятия по видам спорта</p> <p>10.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p> <p>Специальное медицинское отделение</p> <p>11. Учебные занятия по видам спорта</p> <p>11.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p> <p>Специальное медицинское отделение</p> <p>12. Учебные занятия по видам спорта</p> <p>12.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p> <p>Специальное медицинское отделение</p> <p>13. Учебные занятия по видам спорта</p> <p>13.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)</p> <p>Гимнастика</p> <p>Атлетическая гимнастика (занятия в тренажерном зале)</p> <p>Легкая атлетика</p> <p>Пауэрлифтинг и гиревой спорт</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	Специальное медицинское отделение	
Б1.В.ДВ. 06.02	<p>Адаптивные курсы по физической культуре и спорту 1 Цели освоения дисциплины (модуля) Целями освоения дисциплины (модуля) «Адаптивные курсы по физической культуре и спорту» являются:</p> <ul style="list-style-type: none"> формирование физической культуры личности будущего профессионала, востребованного на современном рынке труда; развитие физических качеств и способностей, совершенствование функциональных возможностей организма, укрепление индивидуального здоровья; формирование устойчивых мотивов и потребностей в бережном отношении к собственному здоровью, в занятиях физкультурно-оздоровительной и спортивно-оздоровительной деятельностью; овладение технологиями современных оздоровительных систем физического воспитания, обогащение индивидуального опыта занятий физическими упражнениями с учетом нозологии и показателями здоровья; овладение системой профессионально и жизненно значимых практических умений и навыков, обеспечивающих сохранение и укрепление физического и психического здоровья; освоение системы знаний о занятиях физической культурой, их роли и значении в формировании здорового образа жизни и социальных ориентаций; приобретение компетентности в физкультурно-оздоровительной и спортивной деятельности, овладение навыками творческого сотрудничества в коллективных формах занятий физическими упражнениями; получение знаний и практических навыков самоконтроля при наличии нагрузок различного характера, правил усвоения личной гигиены, рационального режима труда и отдыха; максимально возможное развитие жизнеспособности студента, имеющего устойчивые отклонения в состоянии здоровья, за счет обеспечения оптимального режима функционирования отпущенных природой и имеющихся в наличии его двигательных возможностей и духовных сил, их гармонизации для максимальной самореализации в качестве социально и индивидуально значимого субъекта. В программу входят практические разделы дисциплины, комплексы физических упражнений, виды двигательной активности, методические занятия, учитывающие особенности студентов с ограниченными возможностями здоровья. <p>Программа дисциплины для студентов с ограниченными возможностями здоровья и особыми образовательными потребностями предполагает решение комплекса педагогических</p>	<p><i>Общая трудоемкость дисциплины составляет 0 зачетных единиц</i> 328 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>задач по реализации следующих направлений работы:</p> <p>проведение занятий по физической культуре для студентов с отклонениями в состоянии здоровья, включая инвалидов, с учетом индивидуальных особенностей студентов и образовательных потребностей в области физической культуры;</p> <p>разработку индивидуальных программ физической реабилитации в зависимости от нозологии и индивидуальных особенностей студента с ограниченными возможностями здоровья;</p> <p>разработку и реализацию физкультурных образовательно-реабилитационных технологий, обеспечивающих выполнение индивидуальной программы реабилитации;</p> <p>разработку и реализацию методик, направленных на восстановление и развитие функций организма, полностью или частично утраченных студентом после болезни, травмы; обучение новым способам и видам двигательной деятельности; развитие компенсаторных функций, в том числе и двигательных, при наличии врожденных патологий; предупреждение прогрессирования заболевания или физического состояния студента;</p> <p>обеспечение психолого-педагогической помощи студентам с отклонениями в состоянии здоровья, использование на занятиях методик психоэмоциональной разгрузки и саморегуляции, формирование позитивного психоэмоционального настроения;</p> <p>проведение спортивно-массовых мероприятий для лиц с ограниченными возможностями здоровья по различным видам адаптивного спорта, формирование навыков судейства;</p> <p>организацию дополнительных (внеурочных) и секционных занятий физически-ми упражнениями для поддержания (повышения) уровня физической подготовленности студентов с ограниченными возможностями с целью увеличению объема их двигательной активности и социальной адаптации в студенческой среде;</p> <p>реализацию программ мэйнстриминга в вузе: включение студентов с ограниченными возможностями в совместную со здоровыми студентами физкультурно-рекреационную деятельность, то есть в инклюзивную физическую рекреацию.</p> <p>привлечение студентов к занятиям адаптивным спортом; подготовку студентов с ограниченными возможностями здоровья для участия в соревнованиях; систематизацию информации о существующих в городе спортивных командах для инвалидов и привлечение студентов-инвалидов к спортивной деятельности в этих командах (в соответствии с заболеванием) как в качестве участников, так и в качестве болельщиков.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Дисциплина Адаптивные курсы по физической культуре и спорту входит в базовую часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>"Физическая культура" в объеме средней общеобразовательной школы</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Адаптивные курсы по физической культуре и спорту» обучающийся должен обладать следующими компетенциями:</p> <p>ОК-9 способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности</p> <p>Знать</p> <p>основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;</p> <p>формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;</p> <p>знание технических приемов и двигательных действий базовых видов спорта;</p> <p>современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;</p> <p>основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;</p> <p>технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</p> <p>Уметь</p> <p>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;</p> <p>выполнять физические упражнения разной функционально</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;</p> <p>использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;</p> <p>использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности;</p> <p>анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;</p> <p>анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств;</p> <p>самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</p> <p>Владеть</p> <p>практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике;</p> <p>навыками использования физических упражнений разной функционально направленной в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;</p> <p>практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;</p> <p>техническими приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности;</p> <p>навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;</p> <p>основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;</p> <p>навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Введение</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.1 Физическая культура в общекультурной и профессиональной подготовке обучающихся</p> <p>1.2 Основы техники безопасности при выполнении упражнений</p> <p>2. Общефизическая подготовка и лечебная физическая культура</p> <p>2.1 Оздоровительная гимнастика</p> <p>2.2 Атлетическая гимнастика</p> <p>2.3 Скандинавская ходьба</p> <p>2.4 Общеразвивающие упражнения с предметами и без предметов</p> <p>2.5 Фитнес</p> <p>2.6 Подвижные игры</p> <p>3. Учебные занятия по видам спорта</p> <p>3.1 • волейбол</p> <ul style="list-style-type: none"> • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон <p>4. Общефизическая подготовка и лечебная физическая культура</p> <p>4.1 Оздоровительная гимнастика</p> <p>4.2 Атлетическая гимнастика</p> <p>4.3 Скандинавская ходьба</p> <p>4.4 Общеразвивающие упражнения с предметами и без предметов</p> <p>4.5 Фитнес</p> <p>4.6 Подвижные игры</p> <p>5. Учебные занятия по видам спорта</p> <p>5.1 волейбол</p> <ul style="list-style-type: none"> • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон <p>6. Общефизическая подготовка и лечебная физическая культура</p> <p>6.1 Оздоровительная гимнастика</p> <p>6.2 Атлетическая гимнастика</p> <p>6.3 Скандинавская ходьба</p> <p>6.4 Общеразвивающие упражнения с предметами и без предметов</p> <p>6.5 Фитнес</p> <p>6.6 Подвижные игры</p> <p>7. Учебные занятия по видам спорта</p> <p>7.1 волейбол</p> <ul style="list-style-type: none"> • настольный теннис 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон 8. Общефизическая подготовка и лечебная физическая культура 8.1 Оздоровительная гимнастика 8.2 Атлетическая гимнастика 8.3 Скандинавская ходьба 8.4 Общеразвивающие упражнения с предметами и без предметов 8.5 Фитнес 8.6 Подвижные игры 9. Учебные занятия по видам спорта 9.1 волейбол • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон 10. Общефизическая подготовка и лечебная физическая культура 10.1 Оздоровительная гимнастика 10.2 Атлетическая гимнастика 10.3 Скандинавская ходьба 10.4 Общеразвивающие упражнения с предметами и без предметов 10.5 Фитнес 10.6 Подвижные игры 11. Учебные занятия по видам спорта 11.1 волейбол • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон 12. Общефизическая подготовка и лечебная физическая культура 12.1 Оздоровительная гимнастика 12.2 Атлетическая гимнастика 12.3 Скандинавская ходьба 12.4 Общеразвивающие упражнения с предметами и без предметов 12.5 Фитнес 12.6 Подвижные игры 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>13. Учебные занятия по видам спорта 13.1 • волейбол • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон</p> <p>14. Общефизическая подготовка и лечебная физическая культура 14.1 Оздоровительная гимнастика 14.2 Атлетическая гимнастика 14.3 Скандинавская ходьба 14.4 Общеразвивающие упражнения с предметами и без предметов 14.5 Фитнес 14.6 Подвижные игры</p> <p>15. Учебные занятия по видам спорта 15.1 • волейбол • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон</p> <p>16. Общефизическая подготовка и лечебная физическая культура 16.1 Оздоровительная гимнастика 16.2 Атлетическая гимнастика 16.3 Скандинавская ходьба 16.4 Общеразвивающие упражнения с предметами и без предметов 16.5 Фитнес 16.6 Подвижные игры</p> <p>17. Учебные занятия по видам спорта 17.1 • волейбол • настольный теннис • футбол • баскетбол • дартс • интеллектуальные игры (шашки, шахматы, нарды, уголки) • лыжная подготовка • бадминтон</p>	
Б2	Практики	
Б2.Б	Базовая часть	
Б2.Б.01(У)	Учебная-практика по получению первичных	<i>Общая</i>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности</p> <p>1 Цели практики/НИР</p> <p>Целями учебной практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности по специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин общепрофессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.</p> <p>2 Задачи практики/НИР</p> <p>Задачами учебной практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности являются закрепление на практике знаний, умений и навыков, полученных в процессе теоретического обучения, развитие профессиональных навыков и навыков деловой коммуникации, сбор необходимых материалов для написания отчета по практике.</p> <p>3 Место практики/НИР в структуре образовательной программы</p> <p>Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <ul style="list-style-type: none"> Информатика Введение в специальность Теория информации Организация ЭВМ и вычислительных систем Сети и системы передачи информации Основы информационной безопасности Языки программирования <p>Знания (умения, владения), полученные в процессе прохождения практики/НИР будут необходимы для изучения дисциплин/практик:</p> <ul style="list-style-type: none"> Безопасность сетей ЭВМ 	<p><i>трудоёмкость дисциплины составляет 3 зачетных единицы</i></p> <p>108</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Безопасность систем баз данных Безопасность операционных систем Программно-аппаратные средства обеспечения информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем Техническая защита информации Технология построения защищенных распределенных приложений Информационная безопасность распределенных информационных систем Методы выявления нарушений информационной безопасности, аттестация АИС Криптографические методы защиты информации</p> <p>4 Место проведения практики/НИР Учебная практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности проводится на кафедре «Информатики и информационной безопасности», в лабораториях программно-аппаратных средств обеспечения информационной безопасности, защищенных автоматизированных систем, сетей и систем передачи информации и безопасности сетей ЭВМ ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова»</p> <p>Способ проведения практики/НИР: стационарная Практика/НИР осуществляется дискретно</p> <p>5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями: ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p>Знать - Основные физические явления и процессы, имеющие отношение к профессиональной деятельности - Физические основы функционирования систем обработки и передачи информации.</p> <p>Уметь - Определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач - Анализировать физические явления и процессы формализации и решения профессиональных задач</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <ul style="list-style-type: none"> - основными методами математической формализации - методами анализа физических явлений и процессов при решении профессиональных задач - средствами анализа физических явлений и процессов для формализации и решения профессиональных задач <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - Синтаксис языков программирования высокого уровня (объектно-ориентированное программирование); - Современные технологии и методы программирования; - Показатели качества программного обеспечения; - Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; - Принципы организации документирования разработки, процесса сопровождения программного обеспечения. <p>Уметь</p> <ul style="list-style-type: none"> - Работать с интегрированной средой разработки программного обеспечения; - Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; - Проводить комплексное тестирование и отладку программных систем; - Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; - Проводить выбор эффективных способов решения профессиональных задач; - Планировать разработку сложного программного обеспечения; - Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; автоматизированных систем; <p>Владеть</p> <ul style="list-style-type: none"> - 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. <p>ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации в компьютерных системах, сетях, библиотечных фондах</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные понятия информатики; — Основные способы хранения, обработки и передачи информации; — Основы технологии поиска в современных информационно-поисковых системах; — Значение информации в развитии современного общества. <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — 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. <p>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий</p> <p>Знать</p> <ul style="list-style-type: none"> — принципы построения и функционирования, примеры реализаций современных операционных систем; — принципы работы элементов и функциональных узлов электронной аппаратуры; — типовые схмотехнические решения основных узлов и блоков электронной аппаратуры - Принципы адресации в вычислительных сетях; - Принципы организации межсетевого взаимодействия и межсетевой передачи информации <p>Уметь</p> <ul style="list-style-type: none"> — применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); — работать с современной элементной базой электронной аппаратуры - Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками <p>Владеть</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;</p> <p>— Профессиональным языком и терминологией предметной области</p> <p>— Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей</p> <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - Основы построения систем обработки и передачи информации, их современное состояние развития. -Современные поисковые системы и базы данных в сфере профессиональной деятельности. Язык запросов и организацию поиска научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности - Особенности обработки информации с использованием компьютерных систем <p>Уметь</p> <ul style="list-style-type: none"> - Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками сбора современной научно-технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - политику государства в области обеспечения информационной безопасности - национальные, межгосударственные и международные стандарты в области защиты информации 	

Индекс	Наименование дисциплины	Общая трудоем кость, акад. часов (ЗЕТ)
1	2	3
	<p>- современное состояние рынка труда в области обеспечения информационной безопасности</p> <p>- профессиональный стандарт «Специалист по защите информации в автоматизированных системах»</p> <p>- трудовое законодательство РФ</p> <p>Уметь</p> <p>- анализировать информацию по вопросам национальной и информационной безопасности государства;</p> <p>- соблюдать нормы профессиональной этики</p> <p>Владеть</p> <p>- профессиональной терминологией в области информационной безопасности;</p> <p>- практическими навыками соблюдения норм профессиональной этики</p> <p>Практика включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Подготовительный (ознакомительный). 2. Экспериментально- исследовательский 3. Обработка и анализ полученной информации. 4. Отчетный 	
Б2.Б.02(Н)	<p>Научно-исследовательская работа</p> <p>1 Цели практики/НИР</p> <p>Целями научно-исследовательской работы по специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин, приобретение и развитие необходимых умений и навыков в соответствии с требованиями к уровню подготовки выпускника.</p> <p>2 Задачи практики/НИР</p> <p>Задачами научно-исследовательской работы являются: формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение системы оценок эффективности применяемых мер обеспечения защиты информации</p> <p>3 Место практики/НИР в структуре образовательной программы</p> <p>Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:</p> <p>Анализ рисков информационной безопасности</p> <p>Методы мониторинга информационной безопасности АС</p> <p>Методы проектирования защищенных распределенных информационных систем</p>	<p><i>Общая трудоем кость дисципл ины составл яет 15 зачетны х единицы 540 акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Моделирование систем и процессов защиты информации Управление информационной безопасностью Знания (умения, владения), полученные в процессе прохождения практики/НИР будут необходимы для изучения дисциплин/практик: Подготовка к защите и защита выпускной квалификационной работы Производственная-преддипломная практика Подготовка к сдаче и сдача государственного экзамена</p> <p>4 Место проведения практики/НИР Способ проведения практики/НИР: выездная стационарная Практика/НИР осуществляется дискретно</p> <p>5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями: ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 – цели и задачи моделирования систем и процессов защиты информации; - способы обеспечения информационной безопасности информационных систем; - основные принципы построения моделей систем защиты информации - методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем <p>Уметь</p> <ul style="list-style-type: none"> - 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- проводить мониторинг угроз безопасности информационных систем</p> <p>Владеть</p> <ul style="list-style-type: none"> - 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 <p>ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> <p>Знать</p> <p>Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации. Этапы создания междисциплинарных и инновационных проектов.</p> <p>Уметь</p> <p>Участвовать в деятельности специалистов по ЗИ на предприятии, в учреждении, организации.</p> <p>Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации.</p> <p>Принимать участие в междисциплинарных и инновационных проектах</p> <p>Владеть</p> <p>Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации.</p> <p>Навыками организации и реализации междисциплинарных и инновационных проектов</p> <p>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</p> <p>Знать</p> <p>Основы построения систем обработки и передачи информации, их современное состояние развития.</p> <p>Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.</p> <p>Особенности обработки информации с использованием компьютерных систем</p> <p>Уметь</p> <p>Пользоваться современной научно-технической информацией по</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>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.</p> <p>Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.</p> <p>Владеть</p> <p>Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.</p> <p>Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам.</p> <p>Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.</p> <p>ПК-2 способностью создавать и исследовать модели автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> -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 <p>Уметь</p> <ul style="list-style-type: none"> -строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач -применять различные 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 <p>Владеть</p> <ul style="list-style-type: none"> -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; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите</p> <p>-методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <p>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;</p> <p>Уметь</p> <p>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;</p> <p>Владеть</p> <p>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;</p> <p>навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p> <p>Знать</p> <p>нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов</p> <p>Уметь</p> <p>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;</p> <p>применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности</p> <p>Владеть</p> <p>способностью разрабатывать научно-техническую документацию</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации</p> <p>Знать Средства анализа информационной безопасности; Классификацию систем защиты информации; Средства организации аттестации ВП по требованиям безопасности информации.</p> <p>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.</p> <p>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.</p> <p>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;</p> <p>Уметь выполнять работы по оптимизации схем управления автоматизированной системой; - применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;</p> <p>Владеть навыками определения возможных векторов атаки на автоматизированную систему; и осуществлять выбор средств защиты информации</p> <p>Научно-исследовательская работа включает следующие разделы:</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ol style="list-style-type: none"> 1. Планирование научно-исследовательской работы, включающее ознакомление с тематикой исследовательских работ в области информационной безопасности, выбор темы исследования подготовка литературного обзора 2. Проведение научно-исследовательской работы 3. Составление отчета о научно-исследовательской работе 4. Защита выполненной работы 	
Б2.Б.03(П)	<p>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>1 Цели практики</p> <p>Целями производственной практики по получению профессиональных умений и опыта профессиональной деятельности для специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.</p> <p>2 Задачи практики</p> <p>Задачами производственной практики по получению профессиональных умений и опыта профессиональной деятельности являются закрепление, расширение, углубление и систематизацию знаний, полученных при изучении общепрофессиональных и специальных дисциплин, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.</p> <p>Программа практики по специальности обеспечивает обоснованную последовательность формирования у студентов единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.</p> <p>3 Место практики в структуре образовательной программы</p> <p>Для прохождения практики необходимы знания (умения,</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетных единиц</i></p> <p>216</p> <p><i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>владения), сформированные в результате изучения дисциплин/практик:</p> <ul style="list-style-type: none"> Организация ЭВМ и вычислительных систем Информатика Языки программирования Сети и системы передачи информации Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Основы информационной безопасности Технология построения защищенных распределенных приложений Программно-аппаратные средства обеспечения информационной безопасности Безопасность сетей ЭВМ Безопасность систем баз данных Техническая защита информации Методы выявления нарушений информационной безопасности, аттестация АИС Организационное и правовое обеспечение информационной безопасности Информационная безопасность распределенных информационных систем Безопасность операционных систем Разработка и эксплуатация защищенных автоматизированных систем Методы мониторинга информационной безопасности АС Криптографические методы защиты информации Знания (умения, владения), полученные в процессе прохождения практики будут необходимы для изучения дисциплин/практик: Анализ рисков информационной безопасности Виртуальные сети Защита программного обеспечения Информационная безопасность систем организационного управления Моделирование систем и процессов защиты информации Научно-исследовательская работа Производственная-преддипломная практика Подготовка к сдаче и сдача государственного экзамена Подготовка к защите и защита выпускной квалификационной работы <p>4 Место проведения практики</p> <ul style="list-style-type: none"> Производственная практика по получению профессиональных умений и опыта профессиональной 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>деятельности проводится на базе кафедры «Информатики и информационной безопасности», в лабораториях технических средств защиты информации, защищенных автоматизированных систем, программно-аппаратных средств обеспечения информационной безопасности, сетей и систем передачи информации, безопасности сетей ЭВМ ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», ООО «ММК-Информсервис», ПАО «Магнитогорский металлургический комбинат», и других предприятиях г. Магнитогорска, а также Управление ФСТЭК России по УрФО, г. Екатеринбург.</p> <p>Способ проведения практики: выездная и/или стационарная Практика осуществляется дискретно</p> <p>5 Компетенции обучающегося, формируемые в результате прохождения практики и планируемые результаты обучения</p> <p>В результате прохождения практики обучающийся должен обладать следующими компетенциями:</p> <p>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 - виды нарушителей информационной безопасности <p>Уметь</p> <ul style="list-style-type: none"> - 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 - оценивать потенциал нарушителя информационной безопасности - применять базовую модель угроз ПДн <p>Владеть</p> <ul style="list-style-type: none"> - методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации в автоматизированной системе.</p> <ul style="list-style-type: none"> - навыками применения базовой модели угроз ПДн ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах <p>Знать</p> <ul style="list-style-type: none"> - Порядок разработки политик безопасности; - методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах; <p>Уметь</p> <ul style="list-style-type: none"> - 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. - определить перечень необходимых политик безопасности <p>Владеть</p> <ul style="list-style-type: none"> - методиками проведения анализа рисков информационной безопасности распределенных информационных систем; - методами оценки информационных рисков; - навыками разработки политики информационной безопасности автоматизированных систем. <p>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — Источники и классификацию угроз информационной безопасности; — Основные принципы построения систем защиты информации; — Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. — Методы и порядок проведения аудита защищенности информационно- технологических ресурсов <p>Уметь</p> <ul style="list-style-type: none"> — Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; — Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; — Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем; — Проводить аудит защищенности информационно-технологических ресурсов <p>Владеть</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— Методами выявления угроз информационной безопасности автоматизированных систем;</p> <p>— Методами аудита уровня защищенности АИС.</p> <p>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; - основные средства и методы удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах <p>Уметь</p> <ul style="list-style-type: none"> - разрабатывать и администрировать базы данных в соответствии с требованиями информационной безопасности; -настраивать защиту программного обеспечения с применением дистанционного администрирования -настраивать удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах <p>Владеть</p> <ul style="list-style-type: none"> - методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств; -в полной мере средствами администрирования БД в интегрированных средах СУБД. -средствами удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах -навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах <p>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении</p> <p>Знать</p> <ul style="list-style-type: none"> -основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности - организационные меры защиты информации <p>Уметь</p> <ul style="list-style-type: none"> -анализировать эффективность систем защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>государственной тайны;</p> <ul style="list-style-type: none"> - организовывать и обеспечивать сохранение режима конфиденциальности; - формировать требования к защите информации, содержащейся в информационной системе - определить цели и задачи защиты информации в информационной системе, основные этапы создания системы защиты информации <p>Владеть</p> <ul style="list-style-type: none"> - методами формирования требований по защите объекта; - навыками разработки организационно-распорядительных документов <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - Общие принципы построения современных языков программирования высокого уровня. - Язык программирования высокого уровня (объектно-ориентированное программирование). <p>Уметь</p> <ul style="list-style-type: none"> - 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. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования. - Навыками работы с интегрированной средой разработки программного обеспечения. <p>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - 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; <p>Уметь</p> <ul style="list-style-type: none"> - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <ul style="list-style-type: none"> -навыками работы с нормативными правовыми актами ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий <p>Знать</p> <ul style="list-style-type: none"> -Классификацию современных программных и программноаппаратных СЗИ. -Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ. -Типовые структуры и принципы организации программных и программно-аппаратных СЗИ. <p>Уметь</p> <ul style="list-style-type: none"> -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. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками работы с подсистемами системы информационной безопасности автоматизированной системы. - Навыками администрирования системы ИБ АС. <p>ПК-3 способностью проводить анализ защищенности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> - Критерии оценки эффективности и надежности средств защиты распределенных информационных систем - Принципы построения и функционирования распределенных информационных систем в защищённом исполнении -Мероприятия для обеспечения защиты информации <p>Уметь</p> <ul style="list-style-type: none"> -Анализировать техническую и сопроводительную документацию по обеспечению ИБ. -Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты. -Проводить контроль за событиями безопасности и действиями пользователей в информационной системе -Проводить анализ и оценку функционирования системы защиты информации информационной системы <p>Владеть</p> <ul style="list-style-type: none"> -Навыками выбора средств защиты информации -Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе <p>ПК-4 способностью разрабатывать модели угроз и модели</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>нарушителя информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> -Базовую модель угроз ПДн -Нормативно-методические документы в области моделирования угроз -Способы реализации угроз безопасности информации -Типы нарушителя информационной безопасности в автоматизированных системах -Методику разработки модели угроз <p>Уметь</p> <ul style="list-style-type: none"> -Разрабатывать частную модель угроз автоматизированной системы -Определять актуальные угрозы для автоматизированной системы; -Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите; - Навыками разработки частных моделей угроз <p>ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите; <p>Уметь</p> <ul style="list-style-type: none"> - выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите. -оценить риски информационной безопасности автоматизированной системы <p>Владеть</p> <ul style="list-style-type: none"> - навыками анализа рисков информационной безопасности автоматизированных систем -методиками анализа рисков <p>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> — источники и классификацию угроз информационной безопасности; — основные средства и способы обеспечения информационной 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>безопасности, принципы построения систем защиты информации; — основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; Уметь — анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; — классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; —определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения поддерживать конфигурацию информационной системы и ее системы защиты информации Владеть — навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации — 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 — навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы 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 Уметь -принимать участие в разработке проектов нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности Владеть -навыками разработки научно-техническую документации, научно-технических отчетов по результатам выполненных работ ПК-8 способностью разрабатывать и анализировать проектные</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>решения по обеспечению безопасности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — 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 <p>Уметь</p> <ul style="list-style-type: none"> — разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; — применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем <p>Владеть</p> <ul style="list-style-type: none"> — 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 <p>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - Осуществлять анализ 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 <p>Владеть</p> <ul style="list-style-type: none"> - Способами определения уровней защищенности и доверия 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>программно-аппаратных средств защиты информации</p> <ul style="list-style-type: none"> - 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; - Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - Современные технологии программирования. - Основные виды интегрированных сред разработки программного обеспечения. - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении. - Принципы работы элементов и функциональных узлов электронной аппаратуры; - Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; <p>Уметь</p> <ul style="list-style-type: none"> - 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. - Работать с современной элементной базой электронной аппаратуры; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации</p> <p>- Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.</p> <p>Владеть</p> <p>- Навыками реализации алгоритмов на языках программирования высокого уровня;</p> <p>- Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области.</p> <p>- Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.</p> <p>-Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации;</p> <p>- Методиками проектирования топологии вычислительных сетей;</p> <p>- Навыками настройки сетевого оборудования.</p> <p>ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы</p> <p>Знать</p> <p>- систему организационных мер, направленных на защиту информации ограниченного доступа</p> <p>- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;</p> <p>- уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня</p> <p>Уметь</p> <p>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;</p> <p>-разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала</p> <p>Владеть</p> <p>- владеть навыками разработки политик безопасности различных уровней.</p> <p>-владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации</p> <p>ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p> <p>Знать</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- особенности решений по ЗИ в информационных процессах и системах;</p> <p>- определения рисков ИБ применительно к ОИ с заданными характеристиками;</p> <p>- методы и подходы к реализации системы управления безопасностью АИС;</p> <p>- методы анализа процессов для определения актуальных угроз</p> <p>Уметь</p> <p>- оценивать различные инструменты в области проектирования и управления ИБ;</p> <p>- разрабатывать политики безопасности информации АС;</p> <p>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.</p> <p>Владеть</p> <p>- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.</p> <p>ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы</p> <p>Знать</p> <p>- способы организации обмена данными при помощи технологий RPC, RMC и очередей;</p> <p>- криптографические протоколы обмена информацией;</p> <p>- общий порядок действий по выбору мер защиты информации для их реализации в информационной системе</p> <p>- методы проектирования средств защиты информации;</p> <p>Уметь</p> <p>- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;</p> <p>- разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средства защиты информации АС</p> <p>- выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации</p> <p>Владеть</p> <p>- навыками оформления программной документации по ЕСПД;</p> <p>- методами исследования информационно-технологических ресурсов</p> <p>- навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)</p> <p>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать</p> <ul style="list-style-type: none"> - 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. - Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ. <p>Уметь</p> <ul style="list-style-type: none"> - 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 программных и программно-аппаратных СЗИ. - Применять программные и программно-аппаратные средства обеспечения ИБ. <p>Владеть</p> <ul style="list-style-type: none"> - Техниккой настройки технических средств обеспечения информационной безопасности - Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. - Навыками анализа архитектурно-технических и схмотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. - Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС. <p>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> -уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; - положение о системе сертификации средств защиты информации; -продукцию, которую необходимо сертифицировать; -состав участников системы сертификации и их основные функции; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-этапы сертификации; - требования к проведению испытаний СЗИ; -порядок проведения сертификационных испытаний</p> <p>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.</p> <p>Владеть — нормативно-правовой базой в области сертификации средств защиты информации —навыками проведения испытаний средств защиты информации, ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации</p> <p>Знать — Средства анализа информационной безопасности; — Классификацию систем защиты информации; — Средства организации аттестации по требованиям безопасности информации</p> <p>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.</p> <p>Владеть — Навыками использования средств анализа информационной безопасности; — Навыками проведения аттестации в соответствии с существующими нормативами.</p> <p>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>Знать - перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации;</p> <p>Уметь - применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>проводных сетей построенных на основе неуправляемых коммутаторов;</p> <p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе; <p>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> -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; <p>Уметь</p> <ul style="list-style-type: none"> -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 <p>Владеть</p> <ul style="list-style-type: none"> -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 предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов <p>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - нормативные методические документы ФСТЭК России в области ИБ; - основные принципы создания системы управления информационной безопасностью. - методы реализации системы управления безопасностью 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Уметь</p> <ul style="list-style-type: none"> - проводить оценку информационных рисков, - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС. <p>Владеть</p> <ul style="list-style-type: none"> - навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ. - навыками подготовки документации СУИБ <p>ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. - классификацию информационных систем по требованиям защиты информации. <p>Уметь</p> <ul style="list-style-type: none"> - Определять класс защищенности информационной системы - Принимать участие в реализации 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. - выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы - определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации <p>Владеть</p> <ul style="list-style-type: none"> - Навыками разработки автоматизированных систему с учетом требований ИБ. - Навыками контроля разработки АС с учетом требований ИБ. - Навыками выбора средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации - Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС <p>ПК-21 способностью разрабатывать проекты документов,</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; — 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; <p>Уметь</p> <ul style="list-style-type: none"> — 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 <p>Владеть</p> <ul style="list-style-type: none"> — навыками 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 — навыками разработки организационно-распорядительных документов <p>ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p> <p>Знать</p> <ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя ОИ; - принципы формирования политики информационной безопасности организации. - способы контроля эффективности реализации политики информационной безопасности <p>Уметь</p> <ul style="list-style-type: none"> - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.</p> <p>Владеть</p> <p>- навыками разработки политик безопасности различных уровней. - навыками и методами контроля эффективности сформированной политики информационной безопасности</p> <p>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>Знать</p> <p>- Методы формирования требований по защите информации ограниченного доступа - Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Организационные меры по защите информации ограниченного доступа</p> <p>Уметь</p> <p>- Использовать методы формирования требований по защите информации ограниченного доступа - Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа</p> <p>Владеть</p> <p>- Методами формирования требований по защите информации ограниченного доступа - Навыками анализа методов формирования требований по защите информации ограниченного доступа</p> <p>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <p>- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;</p> <p>Уметь</p> <p>- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации</p> <p>Владеть</p> <p>- навыками определения возможных векторов атаки на</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>автоматизированную систему и осуществлять выбор средств защиты информации;</p> <p>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p> <p>Знать</p> <ul style="list-style-type: none"> - Принципы администрирования баз данных. Средства обеспечения безопасности данных. - Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных <p>Уметь</p> <ul style="list-style-type: none"> - 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 - Выявлять инциденты и реагировать на них - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации <p>Владеть</p> <ul style="list-style-type: none"> - 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. - Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации - Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий <p>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; — Принципы администрирования системы информационной безопасности автоматизированной системы. <p>Уметь</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— Настраивать систему информационной безопасности автоматизированной системы;</p> <p>— Настраивать подсистемы системы информационной безопасности автоматизированной системы;</p> <p>— Самостоятельно администрировать систему информационной безопасности автоматизированной системы.</p> <p>Владеть</p> <p>— Навыками работы с системой информационной безопасности автоматизированной системы;</p> <p>— Навыками работы с подсистемами системы информационной безопасности автоматизированной системы;</p> <p>— Навыками администрирования системы информационной безопасности автоматизированной системы.</p> <p>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы</p> <p>Знать</p> <p>— Способы обработки исключительных ситуаций</p> <p>— Нормативные документы по стандартизации и сертификации программной защиты.</p> <p>— Цели и задачи разработки политики информационной безопасности</p> <p>— Методы и средства анализа достаточности мер по обеспечению ИБ ПО</p> <p>—Порядок контроля (мониторинга) за обеспечением уровня защищенности информации</p> <p>Уметь</p> <p>— Разрабатывать порядок эксплуатации программного обеспечения</p> <p>— Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения</p> <p>— Проводить мониторинг и аудит защищенности ПО</p> <p>—Осуществлять контроль за событиями безопасности и действиями пользователей в информационной системе</p> <p>Владеть</p> <p>— Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО</p> <p>— Методами контроля соблюдения политики учетных записей</p> <p>— Навыками регламентации обслуживания и осуществления модификации программного обеспечения</p> <p>ПК-28 способностью управлять информационной безопасностью автоматизированной системы</p> <p>Знать</p> <p>-методы и средства контроля охраняемых сведений</p> <p>- программные средства, поддерживающие управление</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационной безопасностью -отечественный и зарубежный опыт в области управления информационной безопасностью - основные принципы создания системы управления информационной безопасностью Уметь -разрабатывать политики безопасности для элементов системы ОУ -расследовать инциденты ИБ -разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ -готовить предложения для актуализации организационных мер по защите информационных систем - разрабатывать профили защиты Владеть - терминологией и процессным подходом построения СУИБ. -навыками определения актуальных угроз и применения мер их нейтрализации - навыками составления технических политик безопасности Практика включает в себя следующие разделы: 1. Подготовительный (ознакомительный) 2. Экспериментально- исследовательский 3. Обработка и анализ полученной информации. 4. Отчетный</p>	
Б2.Б.04(П)	<p>Производственная преддипломная практика 1 Цели практики Целями производственной преддипломной практики для специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин базовой и вариативной части ОП, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации. 2 Задачи практики Задачами производственной преддипломной практики являются закрепление, расширение, углубление и систематизацию знаний, полученных при изучении дисциплин базовой и вариативной части, на основе изучения деятельности конкретной</p>	<p><i>Общая трудоемкость дисциплины составляет 6 зачетных единиц</i> 216 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>организации, приобретение практического опыта, а также обобщение и систематизация разделов выпускной квалификационной работы.</p> <p>Программа практики по специальности обеспечивает обоснованную последовательность формирования у обучающихся единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.</p> <p>3 Место практики в структуре образовательной программы</p> <p>Для прохождения практики необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <ul style="list-style-type: none"> Организация ЭВМ и вычислительных систем Информатика Сети и системы передачи информации Основы информационной безопасности Программно-аппаратные средства обеспечения информационной безопасности Техническая защита информации Безопасность сетей ЭВМ Безопасность систем баз данных Информационная безопасность распределенных информационных систем Методы выявления нарушений информационной безопасности, аттестация АИС Безопасность операционных систем Организационное и правовое обеспечение информационной безопасности Тестирование систем защиты информации автоматизированных систем Разработка и эксплуатация защищенных автоматизированных систем Разработка эксплуатационной документации на системы защиты информации автоматизированных систем Основы управленческой деятельности Криптографические методы защиты информации Моделирование угроз информационной безопасности Управление информационной безопасностью Методы мониторинга информационной безопасности АС Информационная безопасность систем организационного управления Защита электронного документооборота 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Защита программного обеспечения Виртуальные сети Анализ рисков информационной безопасности Знания (умения, владения), полученные в процессе прохождения практики будут необходимы для изучения дисциплин/практик: Подготовка к сдаче и сдача государственного экзамена Подготовка к защите и защита выпускной квалификационной работы</p> <p>4 Место проведения практики Производственная практика по получению профессиональных умений и опыта профессиональной деятельности проводится на базе кафедры «Информатики и информационной безопасности», в лабораториях технических средств защиты информации, защищенных автоматизированных систем, программно-аппаратных средств обеспечения информационной безопасности, сетей и систем передачи информации, безопасности сетей ЭВМ ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», ООО «ММК-Информсервис», ПАО «Магнитогорский металлургический комбинат», и других предприятиях г. Магнитогорска, а также Управление ФСТЭК России по УрФО, г. Екатеринбург.</p> <p>Способ проведения практики: выездная и/или стационарная Практика осуществляется дискретно</p> <p>5 Компетенции обучающегося, формируемые в результате прохождения практики и планируемые результаты обучения В результате прохождения практики обучающийся должен обладать следующими компетенциями: ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>Знать</p> <ul style="list-style-type: none"> - 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 - виды нарушителей информационной безопасности <p>Уметь</p> <ul style="list-style-type: none"> - оценивать информационные риски в автоматизированных системах; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- классифицировать и оценивать угрозы безопасности информации;</p> <p>- определять подлежащие защите информационные ресурсы автоматизированных систем;</p> <p>- анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации</p> <p>- оценивать потенциал нарушителя информационной безопасности</p> <p>- применять базовую модель угроз ПДн</p> <p>Владеть</p> <p>- методами выявления угроз безопасности информации в автоматизированных системах;</p> <p>- методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.</p> <p>- навыками применения базовой модели угроз ПДн</p> <p>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах</p> <p>Знать</p> <p>- Порядок разработки политик безопасности;</p> <p>- методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;</p> <p>Уметь</p> <p>- оценивать информационные риски в автоматизированных системах;</p> <p>- выполнять анализ рисков информационной безопасности в распределенных информационных системах;</p> <p>- анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.</p> <p>- определить перечень необходимых политик безопасности</p> <p>Владеть</p> <p>- методиками проведения анализа рисков информационной безопасности распределенных информационных систем;</p> <p>- методами оценки информационных рисков;</p> <p>- навыками разработки политики информационной безопасности автоматизированных систем.</p> <p>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем</p> <p>Знать</p> <p>— Источники и классификацию угроз информационной безопасности;</p> <p>— Основные принципы построения систем защиты информации;</p> <p>— Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— Методы и порядок проведения аудита защищенности информационно- технологических ресурсов</p> <p>Уметь</p> <ul style="list-style-type: none"> — Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; — Участвовать в проведении мониторинга угроз безопасности автоматизированных систем; — Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем; — Проводить аудит защищенности информационно-технологических ресурсов <p>Владеть</p> <ul style="list-style-type: none"> — Методами выявления угроз информационной безопасности автоматизированных систем; — Методами аудита уровня защищенности АИС. <p>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении</p> <p>Знать</p> <ul style="list-style-type: none"> -основные методы организации обеспечения информационной безопасности; - принципы организации обеспечения информационной безопасности - организационные меры защиты информации <p>Уметь</p> <ul style="list-style-type: none"> -анализировать эффективность систем защиты информации и разрабатывать направления ее развития; -организовывать и обеспечивать сохранение режима государственной тайны; - организовывать и обеспечивать сохранение режима конфиденциальности; -формировать требования к защите информации, содержащейся в информационной системе -определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации <p>Владеть</p> <ul style="list-style-type: none"> -методами формирования требований по защите объекта; -навыками разработки организационно-распорядительных документов <p>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p> <p>Знать</p> <ul style="list-style-type: none"> -принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов -принципы и алгоритм принятия решений в нестандартных 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия</p> <p>-о социальных, этнических, конфессиональных и культурных особенностях представителей тех или иных социальных общностей</p> <p>Уметь</p> <p>-работать в коллективе, эффективно выполнять задачи профессиональной деятельности</p> <p>-находить организационно - управленческие решения в нестандартных ситуациях</p> <p>-работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия</p> <p>Владеть</p> <p>-приемами взаимодействия с сотрудниками, выполняющими различные профессиональные задачи и обязанности</p> <p>-навыками находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность</p> <p>-способами и приемами предотвращения возможных конфликтных ситуаций в процессе профессиональной деятельности</p> <p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>Знать</p> <p>-Общие принципы построения современных языков программирования высокого уровня.</p> <p>-Язык программирования высокого уровня (объектно-ориентированное программирование).</p> <p>Уметь</p> <p>-Работать с интегрированной средой разработки программного обеспечения.</p> <p>-Использовать шаблоны классов и средства макрообработки.</p> <p>-Использовать динамически подключаемые библиотеки.</p> <p>-Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.</p> <p>Владеть</p> <p>-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования.</p> <p>-Навыками работы с интегрированной средой разработки программного обеспечения.</p> <p>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать</p> <ul style="list-style-type: none"> -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; <p>Уметь</p> <ul style="list-style-type: none"> -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности <p>Владеть</p> <ul style="list-style-type: none"> -навыками работы с нормативными правовыми актами ПК-2 способностью создавать и исследовать модели автоматизированных систем <p>Знать</p> <ul style="list-style-type: none"> - основные принципы моделирования и виды моделей, требования, предъявляемые к моделям; - методы оценки качества моделей, методы и средства моделирования; - методы исследования моделей автоматизированных систем; - структуру и состав автоматизированных систем управления <p>Уметь</p> <ul style="list-style-type: none"> - применять различные методы моделирования автоматизированных систем; - выбирать методы и средства моделирования подсистем защиты информации; - анализировать и оценивать угрозы информационной безопасности объекта. <p>Владеть</p> <ul style="list-style-type: none"> - навыками анализа информационной инфраструктуры автоматизированной системы; - методами моделирования автоматизированных систем; - основами построения моделей автоматизированных систем; - навыками формализации задач и постановки задач моделирования; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите. <p>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> -Базовую модель угроз ПДн -Нормативно-методические документы в области моделирования угроз 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-Способы реализации угроз безопасности информации -Типы нарушителя информационной безопасности в автоматизированных системах -Методику разработки модели угроз 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 ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы Знать - методологию анализа рисков информационной безопасности; - методики определения информационно-технологических ресурсов, подлежащих защите; Уметь - выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите. -оценить риски информационной безопасности автоматизированной системы Владеть - навыками анализа рисков информационной безопасности автоматизированных систем -методиками анализа рисков ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности 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; Уметь — анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;</p> <ul style="list-style-type: none"> — классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; — определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения <p>поддерживать конфигурацию информационной системы и ее системы защиты информации</p> <p>Владеть</p> <ul style="list-style-type: none"> — навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации — 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 — навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы <p>ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — 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 <p>Уметь</p> <ul style="list-style-type: none"> — разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; — применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем <p>Владеть</p> <ul style="list-style-type: none"> — 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 <p>ПК-9 способностью участвовать в разработке защищенных</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>автоматизированных систем в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> - 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. <p>Уметь</p> <ul style="list-style-type: none"> - Осуществлять анализ 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 <p>Владеть</p> <ul style="list-style-type: none"> - 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; - Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах <p>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</p> <p>Знать</p> <ul style="list-style-type: none"> - Современные технологии программирования. - Основные виды интегрированных сред разработки программного 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обеспечения.</p> <ul style="list-style-type: none"> - Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении. - Принципы работы элементов и функциональных узлов электронной аппаратуры; - Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры - Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; <p>Уметь</p> <ul style="list-style-type: none"> - 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. - Работать с современной элементной базой электронной аппаратуры; - Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации - Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками реализации алгоритмов на языках программирования высокого уровня; - Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области. - Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. - Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации; - Методиками проектирования топологии вычислительных сетей; - Навыками настройки сетевого оборудования. <p>ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - особенности решений по ЗИ в информационных процессах и системах; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- определения рисков ИБ применительно к ОИ с заданными характеристиками;</p> <p>- методы и подходы к реализации системы управления безопасностью АИС;</p> <p>- методы анализа процессов для определения актуальных угроз</p> <p>Уметь</p> <p>- оценивать различные инструменты в области проектирования и управления ИБ;</p> <p>- разрабатывать политики безопасности информации АС;</p> <p>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.</p> <p>Владеть</p> <p>- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.</p> <p>ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы</p> <p>Знать</p> <p>- способы организации обмена данными при помощи технологий RPC,RMC и очередей;</p> <p>- криптографические протоколы обмена информацией;</p> <p>- общий порядок действий по выбору мер защиты информации для их реализации в информационной системе</p> <p>- методы проектирования средств защиты информации;</p> <p>Уметь</p> <p>- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;</p> <p>- разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средства защиты информации АС</p> <p>- выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации</p> <p>Владеть</p> <p>- навыками оформления программной документации по ЕСПД;</p> <p>- методами исследования информационно-технологических ресурсов</p> <p>-навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)</p> <p>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Знать</p> <p>- Способы и средства защиты информации от утечки по</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>техническим каналам и контроля эффективности защиты информации.</p> <ul style="list-style-type: none"> - Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации. - Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ. <p>Уметь</p> <ul style="list-style-type: none"> - 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 программных и программно-аппаратных СЗИ. - Применять программные и программно-аппаратные средства обеспечения ИБ. <p>Владеть</p> <ul style="list-style-type: none"> - Техниккой настройки технических средств обеспечения информационной безопасности - Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. - Навыками анализа архитектурно-технических и схмотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем. - Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС. <p>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> -уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий; - положение о системе сертификации средств защиты информации; -продукцию, которую необходимо сертифицировать; -состав участников системы сертификации и их основные функции; -этапы сертификации; - требования к проведению испытаний СЗИ; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-порядок проведения сертификационных испытаний</p> <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — нормативно-правовой базой в области сертификации средств защиты информации —навыками проведения испытаний средств защиты информации <p>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации</p> <p>Знать</p> <ul style="list-style-type: none"> — Средства анализа информационной безопасности; — Классификацию систем защиты информации; — Средства организации аттестации по требованиям безопасности информации <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — Навыками использования средств анализа информационной безопасности; — Навыками проведения аттестации в соответствии с существующими нормативами. <p>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>Знать</p> <ul style="list-style-type: none"> - перечень инструментов для проведения мониторинга защищенности информации; - базовый функционал инструментов для проведения мониторинга защищенности информации; <p>Уметь</p> <ul style="list-style-type: none"> - применять технические средства для проведения мониторинга беспроводных сетей; - применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Владеть</p> <ul style="list-style-type: none"> - навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе; <p>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p>Знать</p> <ul style="list-style-type: none"> -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; <p>Уметь</p> <ul style="list-style-type: none"> -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 <p>Владеть</p> <ul style="list-style-type: none"> -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 предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов <p>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> - нормативные методические документы ФСТЭК России в области ИБ; - основные принципы создания системы управления информационной безопасностью. - методы реализации системы управления безопасностью <p>Уметь</p> <ul style="list-style-type: none"> - проводить оценку информационных рисков, 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>- обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности;</p> <p>- расследовать инциденты ИБ;</p> <p>- разрабатывать предложения по совершенствованию СУИБ АС.</p> <p>Владеть</p> <p>- навыками расчета и управления рисками ИБ;</p> <p>- навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.</p> <p>- навыками подготовки документации СУИБ</p> <p>ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <p>- Основы организационного и правового обеспечения ИБ.</p> <p>- Основные нормативные и правовые акты в области обеспечения ИБ.</p> <p>- Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ.</p> <p>- классификацию информационных систем по требованиям защиты информации.</p> <p>Уметь</p> <p>- Определять класс защищенности информационной системы</p> <p>- Принимать участие в реализации разработанной АС с учетом требований информационной безопасности.</p> <p>- Готовить сопроводительную документацию к разработанной АС в защищенном исполнении.</p> <p>- Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.</p> <p>- выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы</p> <p>- определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации</p> <p>Владеть</p> <p>- Навыками разработки автоматизированных систему с учетом требований ИБ.</p> <p>- Навыками контроля разработки АС с учетом требований ИБ.</p> <p>- Навыками выбора средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации</p> <p>- Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС</p> <p>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать</p> <ul style="list-style-type: none"> — нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности; — 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; <p>Уметь</p> <ul style="list-style-type: none"> — 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 <p>Владеть</p> <ul style="list-style-type: none"> — навыками 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 — навыками разработки организационно-распорядительных документов <p>ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p> <p>Знать</p> <ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя ОИ; - принципы формирования политики информационной безопасности организации. - способы контроля эффективности реализации политики информационной безопасности <p>Уметь</p> <ul style="list-style-type: none"> - 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 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>частных политик ИБ АС.</p> <p>Владеть</p> <ul style="list-style-type: none"> - навыками разработки политик безопасности различных уровней. - навыками и методами контроля эффективности сформированной политики информационной безопасности <p>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>Знать</p> <ul style="list-style-type: none"> - Методы формирования требований по защите информации ограниченного доступа - Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. - Организационные меры по защите информации ограниченного доступа <p>Уметь</p> <ul style="list-style-type: none"> - Использовать методы формирования требований по защите информации ограниченного доступа - Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа <p>Владеть</p> <ul style="list-style-type: none"> - Методами формирования требований по защите информации ограниченного доступа - Навыками анализа методов формирования требований по защите информации ограниченного доступа <p>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Знать</p> <ul style="list-style-type: none"> - методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы; <p>Уметь</p> <ul style="list-style-type: none"> - применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы - выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации <p>Владеть</p> <ul style="list-style-type: none"> - навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций</p> <p>Знать</p> <ul style="list-style-type: none"> - Принципы администрирования баз данных. Средства обеспечения безопасности данных. - Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных <p>Уметь</p> <ul style="list-style-type: none"> - 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 - Выявлять инциденты и реагировать на них - Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации <p>Владеть</p> <ul style="list-style-type: none"> - 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. - Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации - Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий <p>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы</p> <p>Знать</p> <ul style="list-style-type: none"> — Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем; — Принципы администрирования системы информационной безопасности автоматизированной системы. <p>Уметь</p> <ul style="list-style-type: none"> — Настраивать систему информационной безопасности автоматизированной системы; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— Настраивать подсистемы системы информационной безопасности автоматизированной системы;</p> <p>— Самостоятельно администрировать систему информационной безопасности автоматизированной системы.</p> <p>Владеть</p> <p>— Навыками работы с системой информационной безопасности автоматизированной системы;</p> <p>— Навыками работы с подсистемами системы информационной безопасности автоматизированной системы;</p> <p>— Навыками администрирования системы информационной безопасности автоматизированной системы.</p> <p>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы</p> <p>Знать</p> <p>— Способы обработки исключительных ситуаций</p> <p>— Нормативные документы по стандартизации и сертификации программной защиты.</p> <p>— Цели и задачи разработки политики информационной безопасности</p> <p>— Методы и средства анализа достаточности мер по обеспечению ИБ ПО</p> <p>—Порядок контроля (мониторинга) за обеспечением уровня защищенности информации</p> <p>Уметь</p> <p>— Разрабатывать порядок эксплуатации программного обеспечения</p> <p>— Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения</p> <p>— Проводить мониторинг и аудит защищенности ПО</p> <p>—Осуществлять контроль за событиями безопасности и действиями пользователей в информационной системе</p> <p>Владеть</p> <p>— Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО</p> <p>— Методами контроля соблюдения политики учетных записей</p> <p>— Навыками регламентации обслуживания и осуществления модификации программного обеспечения</p> <p>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</p> <p>Знать</p> <p>- Основы построения систем обработки и передачи информации, их современное состояние развития.</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>-Современные поисковые системы и базы данных в сфере профессиональной деятельности. Язык запросов и организацию поиска научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности</p> <p>- Особенности обработки информации с использованием компьютерных систем</p> <p>Уметь</p> <ul style="list-style-type: none"> - Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам. <p>Владеть</p> <ul style="list-style-type: none"> - Навыками сбора современной научно-технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам. - Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам <p>ПК-3 способностью проводить анализ защищенности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> - Критерии оценки эффективности и надежности средств защиты распределенных информационных систем - Принципы построения и функционирования распределенных информационных систем в защищённом исполнении -Мероприятия для обеспечения защиты информации <p>Уметь</p> <ul style="list-style-type: none"> -Анализировать техническую и сопроводительную документацию по обеспечению ИБ. -Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты. -Проводить контроль за событиями безопасности и действиями пользователей в информационной системе -Проводить анализ и оценку функционирования системы защиты информации информационной системы <p>Владеть</p> <ul style="list-style-type: none"> -Навыками выбора средств защиты информации -Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе <p>ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать</p> <ul style="list-style-type: none"> -нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов <p>Уметь</p> <ul style="list-style-type: none"> -принимать участие в разработке проектов нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации; - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности <p>Владеть</p> <ul style="list-style-type: none"> -навыками разработки научно-техническую документацию, научно-технических отчетов по результатам выполненных работ ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы <p>Знать</p> <ul style="list-style-type: none"> - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня <p>Уметь</p> <ul style="list-style-type: none"> - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; -разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала <p>Владеть</p> <ul style="list-style-type: none"> - владеть навыками разработки политик безопасности различных уровней. -владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации ПК-28 способностью управлять информационной безопасностью автоматизированной системы <p>Знать</p> <ul style="list-style-type: none"> -методы и средства контроля охраняемых сведений - программные средства, поддерживающие управление информационной безопасностью -отечественный и зарубежный опыт в области управления 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационной безопасностью</p> <p>- основные принципы создания системы управления информационной безопасностью</p> <p>Уметь</p> <p>-разрабатывать политики безопасности для элементов системы ОУ</p> <p>-расследовать инциденты ИБ</p> <p>-разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ</p> <p>-готовить предложения для актуализации организационных мер по защите информационных систем</p> <p>- разрабатывать профили защиты</p> <p>Владеть</p> <p>- терминологией и процессным подходом построения СУИБ.</p> <p>-навыками определения актуальных угроз и применения мер их нейтрализации</p> <p>- навыками составления технических политик безопасности</p> <p>Практика включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Подготовительный (ознакомительный) 2. Экспериментально- исследовательский 3. Обработка и анализ полученной информации. 4. Отчетный 	
Б3	Государственная итоговая аттестация	
Б3. Б.01	<p>Подготовка к сдаче и сдача государственного экзамена</p> <p>Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.</p> <p>В соответствии с видами и задачами профессиональной деятельности выпускник на государственной итоговой аттестации должен показать соответствующий уровень освоения следующих компетенций:</p> <ul style="list-style-type: none"> – способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1); – способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2); – способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3); – способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4); – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);</p> <ul style="list-style-type: none"> – способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6); – 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 (ОК-7); – способностью к самоорганизации и самообразованию (ОК-8); – способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9). <ul style="list-style-type: none"> – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1); – способностью 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 (ОПК-2); – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3); – способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4); – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5); – способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6); – способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7); – способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8). – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>в том числе на иностранном языке (ПК-1);</p> <ul style="list-style-type: none"> – способностью создавать и исследовать модели автоматизированных систем (ПК-2); – способностью проводить анализ защищенности автоматизированных систем (ПК-3); – способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4); – способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5); – способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6); – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7); – способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8); – способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9); – 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 (ПК-10); – способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11); – способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12); – способностью участвовать в проектировании средств защиты информации автоматизированной Системы (ПК-13); – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14); – способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15); – способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>(ПК-16);</p> <ul style="list-style-type: none"> – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17); – способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18); – способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19); – способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20); – способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21); – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22); – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23); – способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24); – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25); – способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26); – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27); – способностью управлять информационной безопасностью автоматизированной системы (ПК-28). <p>– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>– способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);</p> <p>– способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);</p> <p>– способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);</p> <p>– способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);</p> <p>Государственный экзамен проводится в два этапа:</p> <ul style="list-style-type: none"> • на первом этапе проверяется сформированность общекультурных компетенций; • на втором этапе проверяется сформированность общепрофессиональных и профессиональных компетенций в соответствии с учебным планом. <p>Первый этап государственного экзамена проводится в форме компьютерного тестирования.</p> <p>Ко второму этапу государственного экзамена допускается обучающийся, получивший оценку «зачтено» на первом этапе. Второй этап государственного экзамена проводится в письменной форме.</p> <p>Второй этап государственного экзамена включает 3 теоретических вопроса и 1 практическое задание.</p> <p>Обучающийся, успешно сдавший государственный экзамен, допускается к выполнению и защите выпускной квалификационной работы.</p>	
Б3.Б.02	<p>Подготовка к защите и защита выпускной квалификационной работы</p> <p>Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.</p> <p>В соответствии с видами и задачами профессиональной деятельности выпускник на государственной итоговой аттестации должен показать соответствующий уровень освоения следующих компетенций:</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> – способностью использовать основы философских знаний для формирования миро-воззренческой позиции (ОК-1); – способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2); – способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования граждан-ской позиции и развития патриотизма (ОК-3); – способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4); – 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 (ОК-5); – способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6); – 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 (ОК-7); – способностью к самоорганизации и самообразованию (ОК-8); – способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9). <ul style="list-style-type: none"> – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1); – способностью 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 (ОПК-2); – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3); – способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4); 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> – способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5); – способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6); – способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7); – способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8). – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1); – способностью создавать и исследовать модели автоматизированных систем (ПК-2); – способностью проводить анализ защищенности автоматизированных систем (ПК-3); – способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4); – способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5); – способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6); – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7); – способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8); – способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9); – 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 (ПК-10); – способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11); – способностью участвовать в проектировании системы 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>управления информационной безопасностью автоматизированной системы (ПК-12);</p> <ul style="list-style-type: none"> – способностью участвовать в проектировании средств защиты информации автома-тизированной Системы (ПК-13); – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты ин-формации (ПК-14); – способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15); – способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16); – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17); – способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18); – способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19); – способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20); – способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21); – способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22); – способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23); – способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24); – способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25); 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<ul style="list-style-type: none"> – способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26); – способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27); – способностью управлять информационной безопасностью автоматизированной системы (ПК-28). – способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1); – способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2); – способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3); – способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4); – способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5); <p>Выполнение и защита выпускной квалификационной работы является одной из форм государственной итоговой аттестации. При выполнении выпускной квалификационной работы, обучающиеся должны показать свои знания, умения и навыки самостоятельно решать на современном уровне задачи своей профессиональной деятельности, профессионально излагать специальную информацию, научно аргументировать и защищать свою точку зрения.</p> <p>Обучающий, выполняющий выпускную квалификационную работу должен показать свою способность и умение:</p> <ul style="list-style-type: none"> – определять и формулировать проблему исследования с учетом ее актуальности; – ставить цели исследования и определять задачи, необходимые для их достижения; – анализировать и обобщать теоретический и эмпирический материал по теме исследования, выявлять противоречия, делать выводы; – применять теоретические знания при решении практических 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>задач; – делать заключение по теме исследования, обозначать перспективы дальнейшего изучения исследуемого вопроса; – оформлять работу в соответствии с установленными требованиями;</p> <p>Защита выпускной квалификационной работы проводится на заседании государственной экзаменационной комиссии и является публичной.</p> <p>Примерный перечень тем выпускных квалификационных работ</p> <ol style="list-style-type: none"> 1. Аудит защищенности информационных ресурсов предприятия. 2. Разработка системы защиты корпоративной сети учебного заведения на основе технологии VipNet. 3. Разработка системы криптографической защиты облачного хранилища данных 4. Разработка средства моделирования угроз безопасности информационной системы на основе теории графов. 5. Разработка автоматизированного комплекса для оценки защищенности от утечки по акустическим каналам. 6. Разработка защищенной информационной системы персональных данных. 7. Разработка автоматизированной системы контроля управления доступом. 8. Разработка защищенной корпоративной сети для топливной компании с применением технологии VPN. 9. Разработка системы защиты для ИСПДн, подключенной к ГИС. 	
ФТД	Факультативы	
ФТД.01	<p>Тестирование систем защиты информации автоматизированных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Тестирование систем защиты информации автоматизированных систем» является формирование у обучающихся понятий о принципах построения и функционирования систем и сетей передачи информации; основных угрозах безопасности информации и модели нарушителя в автоматизированных системах; основных мерах по защите информации в автоматизированных системах; принципах построения средств защиты информации от утечки по техническим каналам; составления методик тестирования систем защиты информации автоматизированных систем; подбора</p>	<p><i>Общая трудоемкость дисциплины составляет 1 зачетных единиц</i> 36 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>инструментальных средств тестирования систем защиты информации автоматизированных систем; составление протоколов тестирования систем защиты информации автоматизированных систем и новейшие технические; программных средствах контроля эффективности мер защиты информации; нормативных правовых актах в области защиты информации; руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Тестирование систем защиты информации автоматизированных систем входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Безопасность операционных систем Сети и системы передачи информации Безопасность сетей ЭВМ Безопасность систем баз данных Программно-аппаратные средства обеспечения информационной безопасности Организация ЭВМ и вычислительных систем Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Методы мониторинга информационной безопасности АС Анализ безопасности программного обеспечения Управление информационной безопасностью Информационная безопасность распределенных информационных систем Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Тестирование систем защиты информации автоматизированных систем»</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>обучающийся должен обладать следующими компетенциями:</p> <p>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — 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 <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспери-ментально-исследовательских работ; — нормативно-правовой базой в области сертификации средств защиты информации <p>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации</p> <p>Знать</p> <ul style="list-style-type: none"> — Средства анализа информационной безопасности; — Классификацию систем защиты информации; — Средства организации аттестации ВП по требованиям безопасности информации. <p>Уметь</p> <ul style="list-style-type: none"> — 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. <p>Владеть</p> <ul style="list-style-type: none"> — Навыками использования средств анализа информационной безопасности; — Навыками проведения экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности; 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>— Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.</p> <p>Дисциплина включает в себя следующие разделы:</p> <p>1. Сертификация средств защиты информации автоматизированных систем</p> <p>1.1 Общие сведения. Организационная структура системы сертификации. Подача заявки на сертификацию</p> <p>1.2 Принятие решения о проведении сертификации средства защиты информации. Сертификационные испытания средства защиты информации</p> <p>1.3 Оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия. Маркирование средств защиты информации. Внесение изменений в сертифицированное средство защиты информации. Переоформление, продление, приостановление и прекращение сертификата</p> <p>2. Аттестации автоматизированных систем с учетом нормативных документов по защите информации</p> <p>2.1 Общие положения. Организационная структура системы аттестации</p> <p>2.2 Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте. Порядок проведения аттестации и контроля</p> <p>2.3 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.</p>	
ФТД.02	<p>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» является формирование у обучающихся понятий эксплуатационной документации, формировании требований и правил обслуживания систем защиты информации, разработки и ведения эксплуатационной документации на системы защиты информации автоматизированных систем и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p>	<p><i>Общая трудоемкость дисциплины составляет 1 зачетных единиц</i></p> <p>36 акад. часов</p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Дисциплина Разработка эксплуатационной документации на системы защиты информации автоматизированных систем входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Безопасность операционных систем Сети и системы передачи информации Безопасность сетей ЭВМ Безопасность систем баз данных Программно-аппаратные средства обеспечения информационной безопасности</p> <p>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Методы мониторинга информационной безопасности АС Анализ безопасности программного обеспечения Управление информационной безопасностью Информационная безопасность систем организационного управления</p> <p>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>Производственная-преддипломная практика</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:</p> <p>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>Знать</p> <ul style="list-style-type: none"> — 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 методы защиты информации в автоматизированных системах. <p>Уметь</p> <ul style="list-style-type: none"> — определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>информации в автоматизированных системах; — Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.</p> <p>Владеть</p> <ul style="list-style-type: none"> — методами анализа защищенности информационной инфраструктуры автома-тизированной системы; — навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач; <p>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p> <p>Знать</p> <ul style="list-style-type: none"> — руководящие и методические документы уполномоченных федеральных орга-нов исполнительной власти по защите информации; — нормативные правовые акты в области защиты информации; — основные методы управления проектами в области информационной безопас-ности. <p>Уметь</p> <ul style="list-style-type: none"> — разрабатывать эксплуатационную документацию на систему защиты автома-тизированных систем; — анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потен-циальных уязвимостей систем защиты информации автома-тизированных сис-тем; — проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности. <p>Владеть</p> <ul style="list-style-type: none"> — методами анализа технической документации информационной инфраструк-туры автоматизированной системы; — навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации. <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> 1. Техническая документация автоматизированных систем в защищенном исполнении <ol style="list-style-type: none"> 1.1 Общие сведения. Назначение технической документации. Требования к технической документации 1.2 Стандарты в области информационных систем. Комплекс стандартов и руководящих документов на автоматизированные системы 	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>1.3 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении.</p> <p>2. Разработка эксплуатационной документации</p> <p>2.1 Общие положения. Состав эксплуатационной документации. Виды и номенклатура эксплуатационных документов. Требования к эксплуатационной документации</p> <p>2.2 Составление руководства пользователя с выделением действий по обеспечению информационной безопасности.</p> <p>2.3 Составление программы и методики испытаний системы защиты автоматизированной системы.</p>	
ФТД.03	<p>Технологическое предпринимательство</p> <p>1 Цели освоения дисциплины (модуля)</p> <p>Целями освоения дисциплины «Технологическое предпринимательство» являются формирование знаний необходимых для решения основных задач, возникающих при реализации инновационных проектов, развитие навыков распознавания источников инновационных возможностей, нахождение способов продвижения инновационного продукта, источников финансирования, формирование навыков подсчета предполагаемой ликвидности и оценки возможных рисков, изучение способов защиты результатов интеллектуальной деятельности (РИД).</p> <p>2 Место дисциплины (модуля) в структуре образовательной программы</p> <p>Дисциплина Технологическое предпринимательство входит в вариативную часть учебного плана образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик:</p> <p>Продвижение научной продукции Экономика Технология командообразования и саморазвития Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:</p> <p>Подготовка к сдаче и сдача государственного экзамена</p> <p>3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</p> <p>В результате освоения дисциплины (модуля) «Технологическое предпринимательство» обучающийся должен обладать следующими компетенциями: ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности</p>	<p><i>Общая трудоемкость дисциплины составляет 3 зачетных единицы</i> 108 <i>акад. часов</i></p>

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Знать основные определения и понятия из области инновационной экономики и технологического предпринимательства; специфику предпринимательской деятельности.</p> <p>Уметь</p> <ul style="list-style-type: none"> – выделять объекты предпринимательской деятельности; – обсуждать способы эффективного решения задач; распознавать эффективное решение от неэффективного; – выявлять и строить типичные модели инновационных задач; – корректно выражать и аргументировано обосновывать экономические положения, связанные с предпринимательской деятельностью <p>Владеть основами применения экономических знаний в сфере предпринимательской деятельности, в том числе алгоритмами оценки эффективности предпринимательской деятельности</p> <p>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>Знать законодательную основу в области предпринимательской деятельности</p> <p>Уметь использовать правовые знания в сфере предпринимательской деятельности</p> <p>Владеть навыками использования законодательной базы при организации предпринимательской деятельности</p> <p>ОК-8 способностью к самоорганизации и самообразованию</p> <p>Знать Комплекс необходимых действий процессов самоорганизации и самообразования, их особенности и технологии реализации, исходя из целей предпринимательской деятельности</p> <p>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.</p> <p>Владеть владеть приемами самоорганизации и способами самообразования при осуществлении предпринимательской деятельности</p> <p>Дисциплина включает в себя следующие разделы:</p>	

Индекс	Наименование дисциплины	Общая трудоемкость, акад. часов (ЗЕТ)
1	2	3
	<p>Раздел 1. Введение в технологическое предпринимательство 1.1 Сущность и свойства инноваций. Классификация инноваций Модели инновационного процесса Роль предпринимателя в инновационном процессе. Правовые основы предпринимательской деятельности 1.2Формирование и развитие команд 1.3.Бизнес-идея, бизнес-модель, бизнес- план 1.4. Маркетинг. Оценка рынка 2. Раздел. Технологическое предпринимательство 2.1Разработка продукта. Product Development. Методы разработки продукта. Оценка технологий. 2.2 Выведение продукта на рынок. Customer Development 2.3. Нематериальные активы. Охрана интеллектуальной собственности 2.4. Трансфер технологий и лицензирование 2.5 Создание и развитие стартапа 2.6 Научно-исследовательские и опытно-конструкторские работы (НИОКР) 3. Раздел Финансирование. Оценка рисков проекта. Представление проекта. Государственная инновационная политика привлекательности проекта 3.1Инструменты привлечения финансирования 3.2Оценка инвестиционной привлекательности проекта 3.3 Риски проекта 3.4 Презентация проекта 3.5 Инновационная экосистема. Государственная инновационная политика</p>	