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

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

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

# 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, 2020

ОП-АИБ-20-1,2

**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** | **История**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины «История» являются:<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина История входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Для освоения этого курса необходимы знания (умения, навыки), сформированные в результате изучения предметов «История России», «Всеобщая история» и «Обществознание» (школьные курсы)<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Философия<br>Правоведение<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «История» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>-Основные проблемы, периоды, тенденции и особенности исторического процесса,<br>-Осознавать место истории России во всемирно-историческом процессе<br>Уметь<br>выражать и обосновывать свою позицию по вопросам, касающимся ценностного отношения к историческому прошлому. | *Общая трудоемкость дисциплины составляет* 4 *зачетных единицы* 144 *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>Навыками межличностной и межкультурной коммуникации, основанные на уважении к историческому наследию и культурным традициям<br>**Дисциплина включает в себя следующие разделы:**<br>1. История в системе социально-гуманитарных наук. Основы методологии исторической науки<br>1.1 Теория и методология исторической науки<br>2. Древнейшая стадия истории человечества<br>2.1 Государство и общество в Древнем мире<br>2.2 Древнерусское государство в IX – XII вв.<br>3. Средневековье как стадия исторического процесса<br>3.1 Средневековье как стадия всемирного исторического процесса.<br>3.2 Русские земли в период раздробленности. Борьба русских земель с иноземными захватчиками<br>3.3 Образование и становление русского централизованного государства в XIV – первой трети XVI вв.<br>4. Россия и мир в XVI-XVIII вв.<br>4.1 Раннее Новое Время: переход к индустриальному обществу<br>4.2 Иван Грозный: реформы и опричнина<br>4.3 Россия в XVII в.<br>4.4 Преобразования традиционного общества при Петре I<br>4.5 Дворцовые перевороты. Правление Екатерины II<br>5. Россия и мир в XIX веке.<br>5.1 Мир XVIII – XIX вв.: попытки модернизации и промышленный переворот.<br>5.2 Россия в первой половине XIX в.<br>5.3 Россия во второй половине XIX в.<br>6. Россия и мир в конце XIX- начале XX вв.<br>6.1 Мир в начале XX века. Первая мировая война<br>6.2 Первая российская революция и ее последствия.<br>6.3 Россия в 1917 г.<br>7. Россия и мир во второй половине XX века<br>7.1 Послевоенное устройство мира (1946 – 1991)<br>7.2 СССР в 1945-1964 гг.: послевоенное восстановление народного хозяйства и попытки реформирования<br>7.3 СССР в 1965 – 1991 гг.<br>8. Россия и мир между двумя мировыми войнами. Вторая мировая война.<br>8.1 Мир между двумя мировыми войнами. Вторая мировая война.<br>8.2 Социалистическая революция и становление советской власти (октябрь 1917-май 1918 гг.). Гражданская война и интервенция<br>8.3 Внутренняя политика СССР в 1920 – 1930-е гг.<br>8.4 СССР в годы Великой Отечественной войны<br>9. Мир на рубеже XX-XXI вв.: пути развития современной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | цивилизации, интеграционные процессы, меж-дународные отношения<br>9.1 Мировое сообщество на рубеже XX – XXI веков<br>9.2 Внутренняя политика Российской Федерации (1991 – 2000-е гг.).<br>10. Экзамен | |
| **Б1.Б.02** | **Иностранный язык**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью освоения дисциплины «Иностранный язык» является:<br>повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования;<br>и 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Иностранный язык входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Дисциплина «Иностранный язык» относится к базовой части образовательной программы (Б1.Б.02).<br>Для изучения дисциплины необходимы знания, умения, владения, сформированные в результате изучения иностранного языка на предыдущем этапе образования.<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Иностранный язык» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского<br>минимума и потенциального словаря, включая термины профилирующей специальности;<br>- определенные приемы, позволяющие совершать познавательную | *Общая трудоемкость дисциплины составляет 7 зачетных единицы 252 акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | и коммуникативную деятельность;<br>- структурные типы простого предложения, грамматические формы и конструкции; порядок слов<br>простого предложения;<br>- виды письменных и устных высказываний в различных коммуникативных ситуациях;<br>- разговорные формулы этикета профессионального общения, приемы структурирования научного<br>дискурса.<br>Уметь<br>- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного<br>языка;<br>- работать с оригинальной литературой научного характера, сопоставлять и определять/ выбирать пути и<br>способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций);<br>- применять полученные знания для преодоления трудностей при переводе с учетом вида перевода, его<br>целей и условий осуществления.<br>Владеть<br>- подготовленной, а также неподготовленной монологической и диалогической речью в пределах<br>изученного языкового материала и в соответствии с избранной специальностью;<br>- терминологией по специальности, а также дискурсивными, лексико-фразеологическими,<br>грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной<br>профессиональной деятельности;<br>- правильно оперировать языковыми средствами английского языка в ситуациях устного общения;<br>- всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое);<br>- письмом в пределах изученного материала (250-300 слов).<br>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<br>Знать<br>основные приемы и методы, связанные с поиском, изучением, обобщением и<br>систематизацией научно-технической информации<br>Уметь<br>использовать основные приемы и методы для поиска, изучения, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | обобщения и<br>систематизации научно-технической информации<br>Владеть<br><br>основными приемами и методами для поиска, изучения, обобщения и<br>систематизации научно-технической информации<br><br>**Дисциплина включает в себя следующие разделы**:<br>1. Я в современном мире<br>1.1 Развитие умений и навыков чтения, говорения и письма по указанной теме<br>1.2 Развитие умений и навыков оперирования лексическими и грамматическими структурами для обеспечения необходимой иноязычной коммуникации по указанной теме<br>2. Ценности образования<br>2.1 Развитие навыков чтения, говорения и письма по теме «Система высшего образования в России и странах изучаемого языка»<br>2.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме<br>3. История научной мысли<br>3.1 Развитие умений и навыков чтения, говорения и письма по теме «Выдающиеся учёные мира» , «Величайшие изобретения человечества»<br>3.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме<br>4. Страна, где я живу<br>4.1 Развитие умений и навыков чтения, говорения и письма по теме:<br>«Российская Федерация: география, политическая система, культура, люди»<br>5. Страны изучаемого языка<br>5.1 Развитие умений и навыков чтения, говорения и письма по теме:<br>« География, культура и традиции страны изучаемого языка» »<br>5.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме<br>6. Современное производство и окружающая среда<br>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» | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 6.2 Развитие умений и навыков оперирования лексическим и грамматическим материалом для обеспечения необходимой иноязычной коммуникации по указанной теме<br>7. Достижения научно-технического прогресса<br>7.1 Развитие умений и навыков чтения, говорения и письма по теме: «Роль и место инновационных технологий в современном мире» ;<br>«Информационные технологии 21-го века»<br>7.2 Диагностика сформированности навыков и умений по всем видам речевой деятельности | |
| **Б1.Б.03** | **Философия**<br>**1 Цели освоения дисциплины (модуля)**<br>- 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.<br>- предоставление необходимого минимума знаний для формирования мировоззренческих оснований научно-исследовательской деятельности;<br>- сформировать представление о специфике философии как способе познания и духовного освоения мира;<br>- сформировать целостное представление о процессах и явлениях, происходящих в неживой и живой природе и общественной жизни;<br>- привить навыки работы с оригинальными и адаптированными философскими текстами;<br>- сформировать представление о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека;<br>- 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;<br>- сформировать представление о ценностных основаниях человеческой деятельности;<br>- определить основания активной жизненной позиции, ввести в круг философских проблем, связанных с областью будущей профессиональной деятельности.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Философия входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | владения), сформированные в результате изучения дисциплин/ практик:<br>Культурология и межкультурное взаимодействие<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Философия» обучающийся должен обладать следующими компетенциями:<br>ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции<br>Знать<br>- основные философские категории и специфику их понимания в различных исторических типах философии и авторских подходах;<br>- основные направления философии и различия философских школ в контексте истории;<br>- основные направления и проблематику современной философии;<br>Уметь<br>- раскрывать смысл выдвигаемых идей, корректно выражать и аргументировано обосновывать положения предметной области знания;<br>- представлять рассматриваемые философские проблемы в развитии;<br>- сравнивать различные философские концепции по конкретной проблеме;<br>- уметь отметить практическую ценность определенных философских положений и выявить основания, на которых строится философская концепция или система;<br>Владеть<br>- навыками работы с философскими источниками и критической литературой;<br>- приемами поиска, систематизации и свободного изложения философского материала и методами сравнения философских идей, концепций и эпох;<br>- способами обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации;<br>- владеть навыками выражения и обоснования собственной позиции относительно современных социогуманитарных проблем и конкретных философских позиций<br><br>**Дисциплина включает в себя следующие разделы**:<br>1.1 Философская картина мира: концепция человека и проблема | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | бытия<br>2.1 История философии: многообразие картин материального мира. Сущность и смысл существования человека. Материальное бытие<br>3.1 Идеальное бытие: сознание, мышление, язык. Гносеология: познавательные отношения человека с объективной реальностью. Методологические проблемы познания.<br>4.1 Динамика общественного развития. Общество. Философская концепция культуры. Философское и нефилософское понимание материи | |
| **Б1.Б.04** | **Экономика**<br>**1 Цели освоения дисциплины (модуля)**<br>- 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, обосновывающих механизм эффективного функционирования экономики;<br>- освоение навыков оценки использования ресурсов предприятия и результатов его деятельности;<br>- формирование у студентов основ экономического мышления;<br>- выработка способности использовать основы экономических знаний в различных сферах жизнедеятельности;<br>- формирование компетенций, необходимых при решении профессиональных задач.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Экономика входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>История<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Технологическое предпринимательство<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Экономика» обучающийся должен обладать следующими компетенциями:<br>ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности<br>Знать | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - основные термины, определения, экономические законы и взаимозависимости на уровне экономики в целом и на уровне отдельного предприятия;<br>- методы исследования экономических отношений на уровне экономики в целом и на уровне отдельного предприятия;<br>- методики расчета важнейших экономических показателей и коэффициентов на уровне экономики в целом и на уровне отдельного предприятия;<br>- теоретические принципы выработки экономической политики на уровне государства и на уровне отдельного предприятия.<br>Уметь<br>- ориентироваться в типовых экономических ситуациях, основных вопросах экономической политики;<br>- использовать элементы экономического анализа в своей профессиональной деятельности;<br>- рационально организовать свое экономическое поведение в качестве агента рыночных отношений,<br>- анализировать и объективно оценивать процессы и явления, осуществляющиеся в рамках национальной экономики в целом и отдельного предприятия в частности.<br>- ориентироваться в учебной, справочной и научной литературе.<br>Владеть<br>- методами и приемами анализа экономических явлений и процессов на уровне экономики в целом и на уровне отдельного предприятия;<br>- практическими навыками использования экономических знаний на других дисциплинах, на занятиях в аудитории и на практике;<br>- на основании теоретических знаний принимать решения на уровне экономики в целом и на уровне отдельного предприятия;<br>- самостоятельно приобретать, усваивать и применять экономические знания, наблюдать, анализировать и объяснять экономические явления, события, ситуации.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Микроэкономика<br>1.1 Введение в экономическую теорию<br>1.2 История экономических учений<br>1.3 Законы рыночной экономики: спрос, предложение, ценообразование<br>1.4 Производитель и потребитель в рыночной экономике<br>1.5 Конкуренция: виды рыночных структур<br>2. Макроэкономика<br>2.1 Закономерности функционирования национальной экономики<br>2.2 Цикличность экономического развития<br>2.3 Экономическая политика государства<br>3. Экономика предприятия | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 3.1 Предприятие как хозяйствующий субъект рыночной экономики<br>3.2 Ресурсы предприятия<br>3.3 Затраты и финансовые результаты деятельности предприятия | |
| **Б1.Б.05** | **Правоведение**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины «Правоведение» являются: формирование у студентов знаний, позволяющих обучающимся ориентироваться в системе законодательства Российской Федерации, давать юридическую оценку реальным событиям общественной жизни.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Правоведение входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>История<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Правоведение» обучающийся должен обладать следующими компетенциями:<br>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности<br>Знать<br>основные правовые понятия;<br>основные источники права;<br>принципы применения юридической ответственности<br>Уметь<br>ориентироваться в системе законодательства;<br>определять соотношение юридического содержания норм с реальными событиями общественной жизни;<br>разрабатывать документы правового характера;<br>приобретать знания в области права;<br>корректно выражать, аргументировано обосновывать свою юридическую позицию<br>Владеть<br>практическими навыками анализа и разрешения юридических | *Общая трудоемкость дисциплины составляет 4 зачетных единицы 144 акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ситуаций;<br>практическими навыками совершения юридических действий в соответствии с законом;<br>навыками составления претензий, заявлений, жалоб по факту неисполнения или ненадлежащего исполнения прав;<br>способами совершенствования правовых знаний и умений путем использования возможностей информационной среды<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>роль правовой информации в развитии современного общества и профессиональной деятельности;<br>виды источников права<br>систему законодательства Российской Федерации<br>Уметь<br>находить и анализировать правовую информацию;<br>использовать правовую информацию при решении конкретных жизненных ситуаций<br>Владеть<br>практическими навыками работы со справочно-поисковыми системами Консультант Плюс и Гарант<br>**Дисциплина включает в себя следующие разделы:**<br>1. Раздел Основы государства и права<br>1.1 Тема Государство: понятие, признаки, формы. Основы конституционного строя Российской Федерации<br>1.2 Тема Право: понятие, источники. Правонарушение и юридическая ответственность. Значение законности и правопорядка в современном обществе. Борьба с коррупцией<br>2. Раздел Основы частного права<br>2.1 Тема Основы гражданского права<br>2.2 Тема Основы семейного права<br>2.3 Тема Основы трудового права<br>3. Раздел Основы публичного права<br>3.1 Тема Основы административного права<br>3.2 Тема Основы уголовного права<br>3.3 Тема Основы экологического права<br>4. Раздел Особенности правового регулирования будущей профессиональной деятельности<br>4.1 Тема Особенности правового регулирования будущей профессиональной деятельности | |
| **Б1.Б.06** | **Культурология и межкультурное взаимодействие**<br>**1 Цели освоения дисциплины (модуля)**<br>– формирование, закрепление и расширение базовых знаний о культурологии как науке и о культурном взаимодействии как предмете культурологии; об основных разделах современного | *Общая трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | культурологического знания и о проблемах и методах их исследования;<br>– 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Культурология и межкультурное взаимодействие входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Иностранный язык<br>История<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Культурология и межкультурное взаимодействие» обучающийся должен обладать следующими компетенциями:<br>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия<br>Знать<br>– суть культурных отношений в обществе, место человека в культурном процессе и жизни общества;<br>– содержание актуальных культурных и общественно значимых проблем современности;<br>– методы и приемы социокультурного анализа проблем современности, основные закономерности культурно-исторического процесса.<br>Уметь<br>– анализировать и оценивать социокультурную ситуацию;<br>– объективно оценивать многообразные культурные процессы и явления;<br>– планировать и осуществлять свою деятельность с позиций сотрудничества, с учетом<br>результатов анализа культурной информации.<br>Владеть<br>– навыками коммуникаций в профессиональной сфере, критики и самокритики, терпимостью; | *составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | – навыками культурного сотрудничества, ведения переговоров и разрешения конфликтов;<br>– навыками толерантного восприятия социальных и культурных различий.<br>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<br>Знать<br>– структуру и содержание межкультурного взаимодействия;<br>– суть ценностно-смысловых отношений в межличностной коммуникации;<br>– материальную и духовную роль культуры в развитии современного общества;<br>– движущие силы и закономерности культурного процесса, многоварантность культурного процесса.<br>Уметь<br>– общаться с представителями других культур, используя приемы межкультурного взаимодействия;<br>– решать задачи межличностного и межкультурного взаимодействия в профессиональной деятельности;<br>– анализировать проблемы культурных процессов;<br>– применять понятийно-категориальный аппарат, основные законы культурологии как гуманитарной науки в профессиональной деятельности;<br>– анализировать и оценивать культурные процессы и явления, планировать и осуществлять свою деятельность с учетом результатов этого анализа.<br>Владеть<br>– навыками межкультурного взаимодействия;<br>– критического восприятия культурно значимой информации;<br>– навыками социокультурного анализа современной действительности;<br>– навыками социального взаимодействия, сотрудничества в позиций расовой, национальной, религиозной терпимости.<br>ОК-1 способностью использовать основы философских знаний для формирования мировоззренческой позиции<br>Знать<br>-культурологические концепции и теории, формирующие представление о различных мировоззренческих позициях их авторов;<br>-сущность понятия культурная картина мира, отражающего особенности мировоззрения личности;<br>-причины формирования различных мировоззренческих позиций, основанных на философских знаниях представителей различных | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | культурных систем<br>Уметь<br>-выстраивать собственную мировоззренческую позицию на основе имеющихся культурно-философских знаний;<br>-обосновывать собственную мировоззренческую позицию;<br>-формировать новые взгляды и представления, основанные на существующих мировоззренческих позициях представителей различных культурных систем<br>Владеть<br>- методом критического анализа в области основ философских знаний с целью формирования собственной мировоззренческой позиции;<br>- приемами убеждения в верности собственной мировоззренческой позиции;<br>- навыком отбора значимых философских знаний для формирования мировоззренческой позиции<br>**Дисциплина включает в себя следующие разделы:**<br>1. Культурология в системе научного знания и проблема межкультурного взаимодействия<br>1.1 Культурология в системе научного знания<br>1.2 Культурогенез и проблема межкультурного взаимодействия<br>1.3 Основные теории происхождения культуры<br>2. Основные понятия культурологии<br>2.1 Основные понятия культурологии<br>2.2 Основные формы и типы культуры<br>2.3 Культура как система знаков<br>3. История культурологических учений<br>3.1 Доклассический и классический периоды развития культурологии<br>3.2 Развитие культурологии во второй половине XIX – XX веках<br>3.3 Типология культур | |
| **Б1.Б.07** | **Технология командообразования и саморазвития**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Дисциплина Технология командообразования и саморазвития входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>История<br>Введение в специальность<br>Культурология и межкультурное взаимодействие<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Правоведение<br>Философия<br>Экономика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Технология командообразования и саморазвития» обучающийся должен обладать следующими компетенциями:<br>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия<br>Знать<br>принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия<br>Уметь<br>находить организационно - управленческие решения в нестандартных ситуациях<br>Владеть<br>умением находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность<br>ОК-8 способностью к самоорганизации и самообразованию<br>Знать<br>способы самоорганизации и развития своего интеллектуального, культурного, духовного, нравственного, физического и профессионального уровня<br>Уметь<br>находить недостатки в своем общекультурном и профессиональном уровня развития и стремиться их устранить;<br>планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения осуществления деятельности<br>Владеть | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | технологиями организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности<br>**Дисциплина включает в себя следующие разделы:**<br>1. Теоретические основы командообразования<br>1.1 Команда как вид групп высшего уровня развития<br>1.2 Формирование команды<br>2. Внутрикомандные процессы и отношения<br>2.1 Распределение ролей и особенности работы в команде<br>2.2 Коммуникации в команде<br>2.3 Управление конфликтами в командах<br>2.4 Управление взаимоотношениями в команде<br>3. Саморазвитие членов команды<br>3.1 Жизненный путь личности и саморазвитие. Индивидуальный коучинг | |
| **Б1.Б.08** | **Безопасность жизнедеятельности**<br>**1 Цели освоения дисциплины (модуля)**<br>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<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина «Безопасность жизнедеятельности» входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Физика<br>Информатика<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Безопасность жизнедеятельности» обучающийся должен обладать следующими компетенциями:<br>ОПК-7 способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | в условиях чрезвычайных ситуаций<br>Знать<br>- основные понятия о приемах первой помощи;<br>- основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности;<br>- характеристики опасностей природного, техногенного и социального происхождения;<br>- государственную политику в области подготовки и защиты населения в условиях чрезвычайных ситуаций<br>Уметь<br>- выделять основные опасности среды обитания человека;<br>- оценивать риск их реализации<br>Владеть<br>- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций<br>**Дисциплина включает в себя следующие разделы:**<br>Раздел 1.<br>1.1 Теоретические основы безопасного и безвредного взаимодействия человека со средой обитания. Первая доврачебная помощь<br>Раздел 2.<br>2.1 Формирование опасностей в производственной среде. Идентификация вредных и опасных факторов технических систем<br>Раздел 3.<br>3.1 Технические методы и средства повышения безопасности и экологичности производственных систем<br>Раздел 4.<br>4.1 Прогнозирование и ликвидация чрезвычайных ситуаций<br>Раздел 5.<br>5.1 Правовые и организационные основы безопасности жизнедеятельности. Управление безопасностью жизнедеятельности | |
| **Б1.Б.09** | **Физика**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Физика входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, | *Общая трудоемкость дисциплины составляет 12 зачетных единицы* ***432*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | владения), сформированные в результате изучения дисциплин/ практик:<br>«Физика», «Математика», «Информатика» на базе среднего (полного) общего образования.<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Основы радиотехники<br>Физические основы передачи информации<br>Электроника и схемотехника<br>Техническая защита информации<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Физика» обучающийся должен обладать следующими компетенциями:<br>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать<br>– основные законы физики, границы применимости этих законов и их связь с явлениями и процессами, происходящими в природе;<br>− методы анализа физических процессов и явлений;<br>− физико-математический аппарат, используемый для описания физических закономерностей<br>Уметь<br>применять физические законы и физико-математический аппарат для формализации описания физических явлений и процессов и решения задач в рамках физики и смежных дисциплин<br>Владеть<br>опытом анализа происходящих физических явлений и процессов и решения физических задач<br>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации<br>Знать<br>методы и подходы к экспериментальному исследованию и моделированию, применяемые в физике и распространяющиеся на другие области знаний<br>Уметь<br>− пользоваться современной аппаратурой для проведения физического эксперимента;<br>− использовать физические модели для описания реальных процессов, с помощью приборов измерять физические величины, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | производить обработку экспериментальных данных и анализировать полученные результаты<br>Владеть<br>− навыками работы с измерительными приборами и оборудованием;<br>− методами проведения физических измерений, расчета величин и анализа полученных данных<br>**Дисциплина включает в себя следующие разделы**:<br>1. Механика<br>1.1 Кинематика поступательного и вращательного движения<br>1.2 Динамика поступательного и вращательного движения<br>1.3 Законы сохранения в механике<br>1.4 Релятивистская механика<br>1.5 Механические колебания и волн<br>2. Молекулярная физика и термодинамика<br>2.1 Молекулярно-кинетическая теория и основы статистической физики<br>2.2 Термодинамика<br>3. Электромагнетизм<br>3.1 Электростатика<br>3.2 Постоянный ток<br>3.3 Магнитостатика<br>3.4 Электромагнитная индукция. Электромагнитные колебания. Переменный ток<br>4. Волновая оптика<br>4.1 Электромагнитное поле. Электромагнитные волны. Волновая природа света.<br>4.2 Взаимодействие света с веществом. Поляризация света<br>4.3 Интерференция света<br>4.4 Дифракция света<br>5. Квантовая оптика<br>5.1 Квантовая оптика. Экспериментальное подтверждение квантовой природы света<br>6. Квантовая физика и физика атома<br>6.1 Элементы квантовой механики<br>6.2 Физика атома<br>6.3 Квантовая статистика. Элементы физики твердого тела.<br>7. Физика ядра и элементарных частиц<br>7.1 Физика атомного ядра. Радиоактивность<br>7.2 Физика элементарных частиц и современная картина мира | |
| **Б1.Б.10** | **Основы управленческой деятельности**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины (модуля) «Основы | *Общая трудоемкость дисципл* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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**.**<br><br>**2 Место дисциплины (модуля) в структуре образовательной программы подготовки специалиста**<br><br>Дисциплина Основы управленческой деятельности входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Технология командообразования и саморазвития<br>Культурология и межкультурное взаимодействие<br>Введение в специальность<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br><br>Производственная-преддипломная практика<br><br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br><br>В результате освоения дисциплины (модуля) «Основы управленческой деятельности» обучающийся должен обладать следующими компетенциями:<br>**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**<br>Знать<br>– понятие и содержание управленческой деятельности | *ины составляет **2** зачетных единицы **72** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Уметь<br>– анализировать внешнюю и внутреннюю среду организации как объекта управленческой деятельности<br>Владеть<br>– основными навыками управленческой деятельности: планирования, организации, мотивации, контроля и коммуникаций<br>**ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности**<br>Знать<br>– основы принятия управленческих решений<br>Уметь<br>– организовывать работу малых коллективов исполнителей<br>Владеть<br>– навыками управления поведением человека в организации<br>**Дисциплина включает в себя следующие разделы:**<br>1.1 Организация как объект управления. Организационно-правовые формы субъектов экономики<br>1.2 Управление как процесс. Планирование, организация, мотивация, контроль как функции управления<br>1.3 Управление поведением человека в организации. Формы власти и влияния.<br>. | |
| **Б1.Б.11** | **Алгебра и геометрия**<br>**1 Цели освоения дисциплины (модуля)**<br>• развитие математического мышления;<br>• формирование навыков решения геометрических задач в различных системах координат;<br>• ознакомление с основами классической и современной алгебры;<br>• ознакомление с различными алгебраическими структурами (полями, векторными пространствами) и их приложениями в решении различных практических задач;<br>• обучение основным алгебраическим методам решения задач, возникающих в других математических дисциплинах и в практике;<br>• воспитание у студентов математической и технической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для современного специалиста.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Алгебра и геометрия входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | практик:<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин: «Алгебра и начала анализа», «Геометрия» в объёме программы средней школы.<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Дискретная математика<br>Теория вероятностей, математическая статистика<br>Математический анализ<br>Исследование операций и теория игр<br>Основы теории оптимизации<br>Математическое моделирование распределенных систем<br>Теория графов и ее приложения<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Алгебра и геометрия» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- основные понятия линейной алгебры и аналитической геометрии<br>- возможности координатного метода для исследования различных геометрических объектов<br>- аналитические способы описания алгебраических структур и геометрических объектов<br>Уметь<br>- сопоставлять реальную задачу с определенной областью математических знаний,<br>- распознавать возможность аналитического решения задачи,<br>- самостоятельно разрабатывать алгоритм решения задачи,<br>- применять типичные математические модели линейной алгебры и аналитической геометрии в профессиональной деятельности;<br>- корректно обосновывать необходимость предложенного метода решения задачи;<br>- формализовать задачу и находить ее решение, используя свойства математических объектов алгебры и геометрии; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - интерпретировать формально (математически) полученный результат<br>Владеть<br>- методами работы с алгебраическими и геометрическими объектами,<br>- методами построения и изучения математических моделей конкретных явлений и процессов для решения расчетных и исследовательских задач;<br>- практическими навыками доказательства суждениий;<br>- умением теоретически обосновывать выводы;<br>- математическими методами описания реальных процессов в профессиональной деятельности.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Линейная алгебра<br>1.1 Матрицы. Определители. Системы линейных алгебраических уравнений.<br>1.2 Линейные пространства. Базис. Евклидовы пространства.<br>1.3 Линейные операторы.<br>1.4 Квадратичные формы.<br>2. Векторная алгебра<br>2.1 Векторы и операции над ними. Скалярное, векторное и смешанное произведение векторов.<br>3. Аналитическая геометрия<br>3.1 Системы координат на плоскости. Прямая на плоскости. Кривые на плоскости.<br>3.2 Кривые второго порядка: окружность, эллипс, гипербола, парабола.<br>3.3 Преобразование координат: параллельный перенос, поворот. Классификация линий 2-го порядка. Приведение уравнений линий 2-го порядка к каноническому виду системы координат в пространстве. Плоскость, прямая в пространстве.<br>3.4 Поверхности второго порядка: цилиндрические, конические и поверхности вращения. Эллипсоид, гиперболоиды, параболоиды.<br>3.5 Классификация поверхностей второго порядка. Приведение к каноническому виду общего уравнения поверхности второго порядка. | |
| **Б1.Б.12** | **Математический анализ**<br>**1 Цели освоения дисциплины (модуля)**<br>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. | *Общая трудоемкость дисциплины составляет 4 зачетны* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Математический анализ входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Алгебра и геометрия<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Дискретная математика<br>Теория вероятностей, математическая статистика<br>Исследование операций и теория игр<br>Математическая логика и теория алгоритмов<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Математический анализ» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- основные положения теории пределов функции;<br>- основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных,<br>- основные понятия теории функций комплексной переменной;<br>- основные методы решения обыкновенных дифференциальных уравнений<br>- основные понятия теории числовых и функциональных рядов<br>Уметь<br>- решать задачи по изучаемым теоретически разделам;<br>- обсуждать способы эффективного решения дифференциальных уравнений и их систем;<br>- определять эффективность решения задачи, полученного с | *х единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | помощью численных методов;<br>- распознавать эффективные результаты обработки экспериментальных данных от неэффективных<br>Владеть<br>- практическими навыками использования математических понятий и методов (изучаемых разделов математики) при решении прикладных задач;<br>- способами оценивания значимости и практической пригодности полученных результатов;<br>- навыками построения и решения математических моделей прикладных задач<br>**Дисциплина включает в себя следующие разделы:**<br>1. Предел и непрерывность функции одной переменной<br>1.1 Понятие множества. Действительные числа и их свойства. Понятие окрестности точки.<br>Понятие функции. Свойства функций<br>1.2 Числовые последовательности. Предел числовой последовательности. Сходимость последовательности. Ограниченные и монотонные последовательности. Простейшие свойства пределов последовательностей. Число е.<br>Предел функции на языке последовательностей. Бесконечно большие, бесконечно малые. Свойства пределов функций. Основные виды неопределенностей<br>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<br>2. Дифференциальное исчисление функции одной действительной переменной<br>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<br>2.2 Дифференцирование неявно заданных, параметрически заданных функций. Логарифмическое дифференцирование<br>2.3 Производные и дифференциалы высших порядков<br>2.4 Основные теоремы дифференциального исчисления: теоремы Ферма, Ролля, Лагранжа, Коши. Формула Тейлора. Формула Тейлора. Применение производных при вычислении пределов. Правило Лопиталя<br>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 | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 3. Интегральное исчисление функции одной действительной переменной<br>3.1 Первообразная функция. Неопределенный интеграл и его основные свойства. Таблица неопределенных интегралов от основных элементарных функций<br>3.2 Методы непосредственного интегрирования. Интегрирование заменой переменной и по частям<br>3.3 Интегрирование рациональных дробей<br>3.4 Интегрирование тригонометрических выражений. Интегрирование иррациональных выражений<br>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<br>3.6 Несобственные интегралы.<br>Признаки сходимости<br>4. Дифференциальное исчисление функций нескольких переменных (ФНП)<br>4.1 Предел и непрерывность ФНП. Основные свойства функций, непрерывных в замкнутой области<br>4.2 Частные производные и производная по направлению. Дифференцируемые функции. Касательная плоскость и нормаль к поверхности. Геометрический смысл дифференциала. Признак дифференцируемости<br>4.3 Производная сложной функции. Частные производные и дифференциалы высших порядков. Дифференцирование неявно заданных функций<br>4.4 Экстремумы ФНП<br>5. Интегральное исчисление функций нескольких переменных (ФНП)<br>5.1 Двойной интеграл и его основные свойства.<br>Сведение двойного интеграла к повторному интегралу. Теорема о среднем значении. Замена переменных, переход в двойном интеграле к полярным координатам<br>5.2 Сведение тройного интеграла к повторному интегралу. Замена переменных, переход в тройном интеграле к цилиндрическим и сферическим координатам<br>5.3 Геометрические и механические приложения кратных интегралов<br>5.4 Криволинейные интегралы I и II ро-да. Вычисление и простейшие свойства криволинейных интегралов. Понятие о поверхностных интегралах<br>6. Обыкновенные дифференциальные уравнения (ОДУ)<br>6.1 Обыкновенные дифференциальные уравнения первого порядка. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Основные определения. Частное и общее решение. Интегральные кривые. Геометрический смысл дифференциального уравнения первого порядка.<br>Методы решения дифференциальных уравнений первого порядка<br>6.2 ДУ высших порядков, допускающие понижение порядка<br>6.3 Линейные дифференциальные уравнения n-го порядка.<br>Линейное однородное уравнение. Фундаментальная система решений. Определитель Вронского.<br>Неоднородное линейное уравнение (ЛНДУ), вид общего решения. Метод вариации произвольных постоянных.<br>Линейное уравнение с постоянными коэффициентами. Характеристическое уравнение. Общее решение<br>6.4 Методы решения систем дифференциальных уравнений (2-го порядка) | |
| **Б1.Б.13** | **Теория вероятностей и математическая статистика**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Теория вероятностей, математическая статистика входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Математический анализ<br>Информатика<br>Теория информации<br>Алгебра и геометрия<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Дискретная математика<br>Исследование операций и теория игр<br>Основы теории оптимизации<br>**3 Компетенции обучающегося, формируемые в результате освоения** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Теория вероятностей, математическая статистика» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>Основные методы исследований, используемых в теории вероятностей и математической статистике<br>Основные законы, правила и определения процессов<br>Уметь<br>Выделять главное, существенное при решении поставленных задач<br>Обсуждать способы эффективного решения поставленных задач<br>Распознавать эффективное решение от неэффективного<br>Объяснять (выявлять и строить) типичные модели поставленных задач<br>Владеть<br>Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат теории вероятностей, математической статистики, в том числе с использованием вычислительной техники.<br>**Дисциплина включает в себя следующие разделы:**<br>1.Теория вероятностей<br>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.<br>1.2.Характеристические функции Вероятностный метод в приложении к зада-чам комбинаторики и теории двоичных функций.<br>2. Математическая статистика<br>2.1. Основные понятия математической статистики. Точечное оценивание параметров распределения. Интервальное оценивание параметров распределения. Проверка статистических гипотез (параметрическая статистика). Проверка статистических гипотез (непараметрическая статистика).<br>2.2. Последовательный статистический анализ. Метод статистических испытаний. Дискретные цепи Маркова | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| **Б1.Б.14** | **Дискретная математика**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Дискретная математика входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Алгебра и геометрия<br>Математический анализ<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Теория графов и ее приложения<br>Математическая логика и теория алгоритмов<br>Исследование операций и теория игр<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Дискретная математика» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>Основные идеи комбинаторики, понятия теории множеств, булевой алгебры, теории конечных автоматов и графов<br>Уметь<br>Применять методы дискретной математики для решения практических задач<br>Выбирать и применять методы дискретной математики и средства вычислительной техники для решения практических задач<br>Владеть<br>Навыками применения математического аппарата дискретной | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | математики для формализации, анализа и выработки решения профессиональных задач с использованием вычислительной техники<br>**Дисциплина включает в себя следующие разделы:**<br>1. Комбинаторика<br>1.1 Понятие выборки. Выборки упорядоченные и неупорядоченные. Размещения, сочетания, перестановки.<br>1.2 Формула бинома Ньютона и следствие из нее.<br>1.3 Алгоритм «Сочетания», алгоритм «Сочетания добавлением/изъятием одного элемента».<br>1.4 Алгоритмы порождения перестановок: «Индуктивный» и «Транспозиция».<br>2. Линейные и циклические коды<br>2.1 Понятие линейного кода. Теорема о числе слов линейного кода. Порождающая и проверочная матрицы линейного кода и их связь<br>2.2 Кодирование линейным кодом. Понятие циклического кода.<br>2.3 Порождающая и проверочная матрицы циклического кода.<br>3. Теория графов<br>3.1 Основные понятия теории графов<br>3.2 Эйлеровы и гамильтоновы графы<br>3.3 Деревья<br>3.4Метрические характеристики графа<br>4. Теория конечных автоматов<br>4.1 Основные понятия теории автоматов<br>4.2 Эквивалентность в автоматах. Эксперименты с автоматами | |
| **Б1.Б.15** | **Математическая логика и теория алгоритмов**<br>**1 Цели освоения дисциплины (модуля):**<br>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 подготовки специалистов к деятельности, связанной с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере.<br>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.<br>**2 Место дисциплины(модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин:<br>«Алгебра и геометрия»,<br>«Математический анализ»,<br>«Дискретная математика»,<br>«Информатика»,<br>«Теория информации»,<br>«Языки программирования».<br>Знания(умения, владения),полученные при изучении данной дисциплины будут необходимы для изучения дисциплин /практик:<br>Исследование операций и теория игр<br>Теория графов и ее приложения<br>Основы теории оптимизации<br>Криптографические методы защиты информации<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины(модуля)и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля)«Математическая логика и теория алгоритмов» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>способы представления и обработки информации с помощью алгоритмов (в том числе, реализованных на современных языках логического программирования),<br>методологию построения математических алгоритмов, методы математического моделирования<br>Уметь<br>корректно применять аппарат математической логики для формализации и решения задач в сфере профессиональной деятельности<br>строить математические алгоритмы, используемые при решении задач в конкретных областях знаний.<br>формулировать полученные результаты в терминах предметной области изучаемого объекта.<br>проводить верификацию программного обеспечения<br>Владеть<br>основными методами математического и алгоритмического моделирования; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | навыками применения вычислительных методов для решения задач профессиональной деятельности<br>навыками построения эффективных алгоритмов с точки зрения теории вычислимости<br>**Дисциплина включает в себя следующие разделы:**<br>1. Пропозициональная логика<br>1.1 Понятие пропозициональной переменной. Пропозициональные формулы. Пропозициональные связки. Система аксиом и теория формального вывода. Свойства формализованного исчисления высказываний.<br>1.2 Логическая равносильность формул. Нормальные формы. Алгоритмы построения нормальных коньюктивных и дизьюнктивных форм.<br>1.3 Нормальные формы. Автоматизация полиномиального разложения. Метод неопределенных коэффициентов. Метод эквивалентных преобразований. Алгоритмы построения полиномиальной нормальной формы.<br>1.4Применение булевых функций для построения релейно-контактных схем. Проектирование контроллеров на базе управляющих элементов булевых функций.<br>2. Булевы функции<br>2.1 Булевы функции n аргументов. Минимизация булевых функций. Графический метод.<br>2.2 Алгоритмы минимизации булевых функций методом Карт Карно. Метод гиперкубов.<br>2.3 Полные системы функций. Базис булевых функций. Теорема Поста о функциональной полноте.<br>3.Логикапредикатов<br>3.1 Основные понятия, связанные с предикатами. Равносильностьиследованиепредикатов.Логическиеиквантор ныеоперациинадпредикатами.<br>3.2 Использование метода резолюций для предикативного вывода. Проблемы разрешения для общезначимости и выполнимости формул.<br>4. Элементы теории алгоритмов<br>4.1 Модели вычислений. Вычислительные парадигмы и задачи<br>5.Конечныеавтоматы<br>5.1 Нормальные алгорифмы Маркова. Алфавит, слова, конкатенация слов, подслова и вхождения. Расширение алфавита и алгорифмы над алфавитом. Нормально вычислимые функции<br>5.2 Машины Тьюринга. ДМТ. НДМТ.<br>5.3 Машины Поста. Эквивалентность моделей и тезис Чёрча—Тьюринга.<br>6. Теория вычислимости<br>6.1 Примитивная рекурсивность. Рекурсивные и примитивно | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | рекурсивные отношения. Ограниченная квантификация и ограниченный поиск. Алгоритмы и разрешимость. Неразрешимые алгоритмические проблемы<br>7.Основы логического программирования<br>7.1 Основные конструкции языка программирования Пролог. Рекурсивное программирование.<br>7.2Метод отсечения и отката. Метод повтора. Списки и их использование. Вычислительная модель логических программ<br>8. Алгоритмы параллельного программирования<br>8.1 Этапы проектирования алгоритмов в парадигме параллельного программирования. Виды параллелизма. Максимальный теоретический выигрыш. Закон Амдала. Максимально допустимое ускорение Закон Густафсона-Барсиса.<br>9.Алгоритмыгенетическогопрограммирования<br>9.1 Концепция построения генетического алгоритма. Генетические операторы. Концептуальные вопросы сферы применения, преимуществ и недостатков ГА.<br>10. Верификация программ<br>10.1 Правильные программы. Императивные программы. Задача верификации программ. Логика Хоара. Автоматическая проверка правильности программ<br>10.2 Верификация распределенных программ. Логика линейного времени PLTL. Размеченные системы переходов. Задача верификации моделей программ. | |
| **Б1.Б.16** | **Теория информации**<br>**1 Цели освоения дисциплины (модуля)**<br>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. 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Теория информации входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Алгебра и геометрия | *Общая трудоемкость дисциплины составляет **5** зачетных единицы **180** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Организация ЭВМ и вычислительных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Безопасность сетей ЭВМ<br>Физические основы передачи информации<br>Техническая защита информации<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Теория информации» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- основы теории информации;<br>- способы измерения количественных характеристик информации;<br>- способы измерения качественных характеристик информационных систем;<br>- основные методы эффективного кодирования;<br>- основные методы помехозащищенного кодирования;<br>Уметь<br>- применять основные постулаты теории информации;<br>- применять современные методы теории информации для решения практических задач;<br>- применять знания, полученные в ходе освоения дисциплины при работе над междисциплинарными и инновационными проектами;<br>- применять методы эффективного кодирования;<br>- применять методы помехозащищенного кодирования;<br>Владеть<br>- профессиональным языком предметной области знания;<br>- современными методиками кодирования;<br>- методиками оценки эффективности алгоритмов сжатия;<br>- методиками оценки эффективности алгоритмов помехоустойчивого кодирования;<br>**Дисциплина включает в себя следующие разделы**:<br>1. Основы теории информации<br>1.1 Возникновение теории информации. Системы передачи информации. Основные понятия. Задачи и постулаты прикладной теории информации. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1.2 Количественная оценка информации. Энтропия. Свойства энтропии. Энтропия при непрерывном сообщении. Условная энтропия. Взаимная энтропия. Избыточность информации. Коэффициенты сжатия и избыточности.<br>2. Методы кодирования, основанные на статистических параметрах.<br>2.1 Методы архивации. Кодирование символами переменной длинны (алгоритм Хаффмана). Кодирование изображения, звука и видео (метод Лемпеля - Зива). Эффективное кодирование. Двоично-десятичные коды. Метод Шеннона-Фано. Метод Хаффмана.<br>3. Помехоустойчивые коды<br>3.1 Кодирование информации для канала с помехами. Разновидность помехоустойчивых кодов. Общие причины использования избыточности. Разрешенные и запрещенные кодовые комбинации. Кодовое расстояние. Матрица<br>3.2 Исправление одиночных ошибок. Контроль по нечетности (четности). Линейные коды. Основные определения. Построение двоичного группового кода.<br>3.3 Коды Хемминга. Обнаружение одиночных ошибок. Исправление одиночных или обнаружение двойных ошибок. Обнаружение ошибок<br>4. Циклические коды.<br>4.1 Определение проверочных равенств. Максоритарное декодирование групповых кодов. Матричное представление линейных кодов. Технические средства кодирования и декодирования<br>4.2 Построение циклических кодов. Порождающий многочлен. Методы образования циклического кода. Технические средства кодирования и декодирования | |
| **Б1.Б.17** | **Информатика**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Информатика» является повышение исходного уровня владения информационными технологиями, 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.<br>Специальная цель дисциплины: формирование представлений об основных принципах информатики, сферах ее применения, перспективах развития, способах функционирования и использования информационных технологий решения задач.<br>Приоритетными объектами изучения информатики являются информационные системы, связанные с информационными | *Общая трудоемкость дисциплины составляет **11** зачетных единицы **396** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | процессами, и информационные технологии, рассматриваемые с позиций системного подхода.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Информатика входит в базовую часть учебного плана образовательной программы.<br>Для освоения дисциплины обучающиеся используют знания, умения и компетенции, сформированные в ходе изучения базового курса «Информатика» в объеме средней общеобразовательной школы.<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Языки программирования<br>Информационные технологии. Базы данных<br>Теория информации<br>Сети и системы передачи информации<br>Технологии и методы программирования<br>Основы теории оптимизации<br>Основы информационной безопасности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Информатика» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>─ Классификацию современных компьютерных систем;<br>─ Классификацию системного и прикладного программного обеспечения;<br>─ Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.<br>Уметь<br>─ Пользоваться расчетными формулами, таблицами, компьютерными программами при решении профессиональных задач;<br>─ Применять офисные приложения (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов) в профессиональной деятельности;<br>─ Эффективно использовать современные компьютерные | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | технологии для решения профессиональных задач.<br>Владеть<br>─ Навыками работы с реляционными системами управления базами данных при решении профессиональных задач;<br>─ Навыками проектирования и реализации алгоритмов для решения профессиональных задач;<br>─ Навыками создания, отладки и выполнения программ интегрированных сред разработки офисных приложений.<br>ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах<br>Знать<br>─ Основные понятия информатики;<br>─ Основные способы хранения, обработки и передачи информации;<br>─ Основы технологии поиска в современных информационно-поисковых системах;<br>─ Значение информации в развитии современного общества.<br>Уметь<br>─ Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет;<br>─ Применять функции офисных приложений для организации поиска информации по заданным критериям;<br>─ Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач.<br>Владеть<br>─ Навыками использования современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах при решении профессиональных задач;<br>─ Навыками построения запросов для организации поиска информации в компьютерных системах, сетях, библиотечных фондах.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Основные понятия и сущность информационных ресурсов. Роль и значение информационных ресурсов в развитии информационных технологий и в информатизации общества<br>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<br>2. Операционные системы. Системное и прикладное программное обеспечение. Современные компьютерные системы.<br>2.1 Системное и прикладное программное обеспечение. Обзор | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | существующих операционных систем, их достоинства и недостатки. Операционная система как виртуальная машина. Операционная система как менеджер ресурсов. ОС WINDOWS, основные концепции.<br>2.2 Программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска).<br>2.3 Классификация современных компьютерных систем. Слои программного обеспечения компьютерной системы. Классификация прикладного программного обеспечения. Основные утилиты.<br>3. Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.<br>3.1 Технические средства реализации информационных процессов. Структура вычислительной системы. Основные характеристики современных компьютеров. Периферийное оборудование.<br>4. Обеспечение безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).<br>4.1 Основы защиты информации. Антивирус как средство защиты информации. Классификация вирусов, основные различия, проявления. Антивирусные программы.<br>4.2 Архивация данных. Восстановление данных<br>5. Типовые структуры и принципы организации компьютерных сетей<br>5.1 Локальные и глобальные сети ЭВМ. Понятие локальных и глобальных сетей. Общие понятия и принципы функционирования сетей. Модель компьютер-ной связи. Глобальная сеть Интернет. Службы Интернета и их назначение. Защита информации в сети.<br>6. Работа с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами под-готовки презентационных материалов)<br>6.1 Средства представления и приемы обработки текстовой информации. Текстовый процессор Word. Основные приемы 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.<br>6.2 Средства представления и приемы обработки презентационных материалов. Этапы и правила создания презентации, редактирование, форматирование, вставка графики и анимации, использование специальных эффектов.<br>6.3 Средства представления и алгоритмы обработки числовой | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>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».<br>7. Использование языков, систем и инструментальных средств программирования в профессиональной деятельности. Алгоритмизация и программирование. Языки программирования высокого уровня.<br>7.1 Автоматизация работы в EXCEL. Макропрограммирование в MS EXCEL, основные понятия, способы написания.<br>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.<br>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.<br>7.4 Организация человеко-машинного интерфейса. Работа с формами и элементами управления. Программирование обработчиков событий.<br>8. Применение достижений современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации.<br>8.1 Информационные системы. Структура и классификация ИС, специализированные ИС. Информационные системы, используемые в предметной области. Основные модели данных. СУБД, общее понятие, классификация.<br>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. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 9. Использование библиотек прикладных программ для решения прикладных математических задач.<br>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.<br>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. | |
| **Б1.Б.18** | **Исследование операций и теория игр**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью курса является ознакомление студентов с основными принципам построения, применения и анализа математических моделей и их использования при разработке конкретных проектов.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина «Исследование операций и теория игр» входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Алгебра и геометрия Математический анализ Дискретная математика<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Основы теории оптимизации<br>Математическое моделирование распределенных систем<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Исследование операций и теория игр» обучающийся должен обладать следующими компетенциями:<br>ОПК-2 Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической | *Общая трудоемкость дисциплины составляет 4 зачетных единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники<br>Знать<br>Основные методы исследования операций и теории игр<br>Определения основных понятий, называет их структурные характеристики<br>Основные законы, правила и определения процессов<br>Уметь<br>Выделять главное, существенное при решении поставленных задач<br>Обсуждать способы эффективного решения поставленных задач<br>Распознавать эффективное решение от неэффективного<br>Владеть<br>Методами исследования операций и теории игр при разработке и исследования моделей информационно- технологических ресурсов<br>Методиками обобщения результатов решения, экспериментальной деятельности<br>**Дисциплина включает в себя следующие разделы:**<br>1. Основные понятия и методологические основы исследования операций<br>1.1. Введение в исследование операций. Основные понятия и методологические основы исследования операций<br>1.2.Методика определения полезности.<br>Принятие решений в различных условиях.<br>2.Задачи массового обслуживания в исследовании операций<br>2.1. Введение в теорию массового обслуживания. Задачи массового обслуживания в рамках исследования операций<br>3. Элементы теории игр<br>3.1. Введение в теорию игр. Матричные игры. Решение матричных игр в чистых стратегиях. Принцип минимакса и максимина. Доминирующие стратегии.<br>3.2. Решение матричных игр в смешанных стратегиях<br>3.3. Игры с природой. Принятие решений в условиях неопределенности. Принятие решений в условиях риска | |
| **Б1.Б.19** | **Теория графов и ее приложения**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Дисциплина Теория графов и ее приложения входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Дискретная математика<br>Математический анализ<br>Языки программирования<br>Теория информации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Криптографические методы защиты информации<br>Методы выявления нарушений информационной безопасности<br>Моделирование угроз информационной безопасности<br>Моделирование систем и процессов защиты информации<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>Научно-исследовательская работа<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Теория графов и ее приложения» обучающийся должен обладать следующими компетенциями:<br>Структурный<br>элемент<br>компетенции<br>Планируемые результаты обучения<br>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Знать<br>-Правила, процедуры, практические приемы, руководящие принципы, методы, средства для построения модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>-Методы и средства разработки моделей на основе теории графов<br>Уметь<br>-Использовать технологии автоматизированного проектирования информационных систем<br>-Применять методы теории графов для построения модели нарушителя в автоматизированных системах | ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>-Навыками применения графовых алгоритмов для определения ресурсов, необходимых для обеспечения безопасности информационной системы<br>-Методами построения моделей для контроля эффективности мер защиты информации<br>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<br>Знать<br>-Основы применения теории графов при решении задач на ЭВМ<br>Способы классификации и виды графов<br>направления развития теории графов<br>-Новые технологии применения теории графов в моделировании предметных областей<br>-связи теории графов с другими предметами, различные информационные технологии, используемые в теории графов<br>Уметь<br>-Применять методы теории графов при решении задач на ЭВМ<br>-Самостоятельно приобретать знания и применять теорию графов при решении задач на ЭВМ<br>-Классифицировать задачи теории графов по степени сложности и применять соответствующие алгоритмы для решения задач<br>Владеть<br>-Методологическими основами формирования изучения графов и их свойств при исследовании и построении систем<br>-Приемами исследования проблем области теории графов, возникающих в различных сферах человеческой деятельности<br>-Навыками разработки и реализации наилучшего решения для поставленной задачи<br>-Навыками решения оптимизационных задач теории графов и задач сетевого планирования<br>**Дисциплина включает в себя следующие разделы:**<br>1. Машинное представление графов<br>1.1 Способы машинного представления графов. Структуры языков программирования высокого уровня для хранения и обработки информации в представлении графовых стуктур. Виды графов, подграфы, операции над графами.<br>2. Обходы графов<br>2.1 Связность, компоненты связности. Маршруты, цепи, пути, циклы. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 2.2 Обходы графов: виды обходов, реализация обходов.<br>3. Каркасы и фундаментальные множества<br>3.1 Каркасы графа. Матрица Кирхгофа. Способы построения каркасов. Алгоритмы поиска каркаса минимального веса<br>3.2 Цикломатическое число графа. Фундаментальное множество (базис) циклов графа.<br>4. Компоненты сильной связности<br>4.1 Теорема Менгера. k- связность графа. Алгоритм нахождения компонент сильной связности графа. Применение алгоритма поиска компонент двусвязности для орпеделения надежности сетей связи.<br>5. Разрезания и раскраска графов<br>5.1 Понятие разреза. Задача о разрезании графа. Разрезание различных видов графов. Понятие раскраски, хроматиеческого числа.<br>5.2 Задача о вершинной раскраске, о раскраске граней, их связь. Оценка хроматического числа для некоторых видов графов.<br>6. Оптимизационные задачи на графах<br>6.1 Поиск кратчайших путей. Алгоритмы Форда-Беллмана, Флойда, Дейкстры, поиск пути в бесконтурном графе.<br>6.2 Задача коммивояжера.<br>6.3 Сетевое планирование. Задача о максимальном потоке.<br>7. Прикладные задачи теории графов<br>7.1 Применение графов для задач программирования, графы как модели программ, процессов, информационных структур.<br>7.2 Построение модели внутреннего нарушителя с применением теории графов.<br>7.3 Применении теории графов к моделированию СЗИ и управлению рисками информационной безопасности<br>8. Укладка графов<br>8.1 Задачи визуализации графов. Задачи плоской укладки графа. Теорема Понтрягина-Куратовского | |
| **Б1.Б.20** | **Языки программирования**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Языки программирования» является изучение языков программирования высокого уровня и формирования у обучающихся навыков их практического применениях 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет* ***9*** *зачетных единицы* ***324*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Дисциплина Языки программирования входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Организация ЭВМ и вычислительных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Технологии и методы программирования<br>Основы теории оптимизации<br>Математическое моделирование распределенных систем<br>Криптографические методы защиты информации<br>Тестирование систем защиты информации автоматизированных систем<br>Защита программного обеспечения<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Языки программирования» обучающийся должен обладать следующими компетенциями:<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>Общие принципы построения современных языков программирования высокого уровня.<br>Общие принципы использования современных языков программирования высокого уровня.<br>Язык программирования высокого уровня (объектно-ориентированное программирование).<br>Уметь<br>Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования.<br>Проводить комплексное тестирование и отладку программных систем.<br>Работать с интегрированной средой разработки программного обеспечения.<br>Использовать шаблоны классов и средства макрообработки.<br>Использовать динамически подключаемые библиотеки.<br>Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.<br>Проектировать и кодировать алгоритмы с соблюдением требований | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | к качественному стилю программирования.<br>Владеть<br>Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования.<br>Навыками работы с интегрированной средой разработки программного обеспечения.<br>Навыками проектирования программного обеспечения с использованием средств автоматизации.<br>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<br>Знать<br>Способы разработки сложного программного обеспечения.<br>Эффективные способы реализации структур данных и конкретных алгоритмов при решении различных задач.<br>Требования, предъявляемые к разработке внешних спецификаций, для разрабатываемого программного обеспечения.<br>Уметь<br>Планировать разработку сложного программного обеспечения.<br>Проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении различных задач.<br>Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения.<br>Владеть<br>Навыками разработки типового программного обеспечения.<br>Навыками разработки внешней спецификации для разрабатываемого программного обеспечения.<br>Навыками разработки сложного программного обеспечения.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Методики разработки программ<br>1.1 Структурное программирование. Модульное программирование. Объектно-ориентированное программирование.<br>1.2 Стандарты построения блок-схем. Представление типовых алгоритмов в виде блок-схем. Среда программирования.<br>2. Языки программирования<br>2.1 Классификация языков программирования<br>2.2 Платформа .NET. Концепция языка программирования C#<br>2.3 Среда быстрой разработки приложений Visual Studio<br>3. Основы языка программирования C#<br>3.1 Структура программы C#. Типы данных. Создание консольных приложений<br>3.2 Функции и процедуры. Математические вычисления<br>3.3 Условный оператор. Оператор выбора. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 3.4 Операторы цикла<br>3.5 Массивы и строки. Создание форм. Элементы управления форм для работы с массивами<br>4. Организация взаимодействия приложения с пользователем<br>4.1 Перехват и обработка ошибок. Обработка особых ситуаций<br>4.2 Обработка диалога с пользователем<br>5. Технологии работы в C#<br>5.1 Способы работы с файлами. Создание файловых переменных. Извлечение данных из файлов. Сохранение данных в текстовый файл<br>5.2 Классы: Основные понятия. Иерархии классов<br>5.3 Интерфейсы и структурные типы<br>5.4 Динамическое распределение памяти. Динамические структуры данных<br>5.5 Сборки, библиотеки, директивы<br>5.6 Программирование под Windows. Введение в графику<br>6. Создание пользовательских приложений<br>6.1 Правила создания пользовательских приложений под Windows | |
| **Б1.Б.21** | **Технологии и методы программирования**<br>**1 Цели освоения дисциплины (модуля)**<br>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 программирования» рассматривает основные подходы к проектированию программных средств, освоении методологий структурного и объектно-ориентированного программирования, а также методов тестирования и отладки программ.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Технологии и методы программирования входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Языки программирования<br>Информационные технологии. Базы данных<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Криптографические методы защиты информации<br>Тестирование систем защиты информации автоматизированных | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144**акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | систем<br>Защита электронного документооборота<br>Управление информационной безопасностью<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Технологии и методы программирования» обучающийся должен обладать следующими компетенциями:<br>Структурный<br>элемент<br>компетенции<br>Планируемые результаты обучения<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>Язык программирования высокого уровня (объектно-ориентированное программирование);<br>Современные технологии и методы программирования;<br>Показатели качества программного обеспечения;<br>Методологии и методы проектирования программного обеспечения;<br>Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;<br>Принципы организации документирования разработки, процесса сопровождения программного обеспечения.<br><br>Уметь<br>Работать с интегрированной средой разработки программного обеспечения;<br>Использовать динамически подключаемые библиотеки;<br>Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;<br>Использовать шаблоны классов и средства макрообработки;<br>Проводить комплексное тестирование и отладку программных систем;<br>Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;<br>Проводить выбор эффективных способов реализации профессиональных задач;<br>Планировать разработку сложного программного обеспечения;<br>Формировать требования и разрабатывать внешние спецификации | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | для разрабатываемого программного обеспечения;<br>автоматизированных систем;<br>Владеть<br>Основными навыками проектирования программного обеспечения с использованием средств автоматизации.<br>Навыками программирования различными стилями.<br>Навыками разработки программной документации.<br>Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.<br>Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.<br>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<br>Знать<br>Области и особенности применения языков программирования высокого уровня;<br>Основные виды интегрированных сред разработки программного обеспечения.<br>Способы обработки исключительных ситуаций;<br>Современные технологии и методы программирования, предназначенные для создания прикладных программ.<br>Уметь<br>Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач;<br>Работать с основными средами интегрированной разработки программного обеспечения;<br>Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;<br>Реализовывать разработанную структуру классов для задач предметной<br>Владеть<br>Навыками реализации алгоритмов на языках программирования высокого уровня;<br>Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области.<br>Технологиями программирования распределенных автоматизированных систем;<br>Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **Дисциплина включает в себя следующие разделы:**<br>1. Введение в технологии программирования<br>1.1 Языки и парадигмы программирования. Инструментальные средства для разработки программных средств. Компиляторы и интерпретаторы. Классификация технологических подходов. Коллективная разработка ПО.<br>1.2 Жизненный цикл программных средств. Модели жизненного цикла. Каскадная, инкрементная и спиральная модели. Понятие качества программного средства.<br>2. Проектирование и разработка архитектуры<br>2.1 Основные подходы к проектированию ПО.<br>2.2 Тестирование и отладка ПО. Документация и сопровождение ПО.<br>3. Преимущества языка Python<br>3.1 Особенности языка. Преимущества языка Python.<br>4. Язык программирования Python<br>4.1 Основные конструкции и базовые типы<br>4.2 Операторы ветвления, циклы. Функции.<br>4.3 Структуры данных: списки (lists), кортежи (tuples) и словари (dictionaries).<br>4.4<br>Объектно-ориентированное программирование на Python. Классы и экземпляры. Наследование в Python. Композиция классов. Классы исключений и их обработка. Генерация исключений<br>4.5 Работа с файловой системой.<br>4.6 Функциональное программирование в Python. Замыкания. Декораторы. Генераторы.<br>4.7 Обработка исключений.<br>5. Многопоточное и асинхронное программирование<br>5.1 Процесс и его характеристики. Создание процессов. Создание потоков<br>5.2 Синхронизация потоков. Глобальная блокировка интерпретатора.<br>5.3 Сокеты, клиент-сервер.Таймауты и обработка сетевых ошибок. Обработка нескольких соединений. Генераторы и сопрограммы.<br>5.4 Работа с asyncio. Клиент для отправки метрик. Сервер для приема метрик.<br>5.5 Работа с asyncio. Клиент для отправки метрик. Сервер для приема метрик. | |
| **Б1.Б.22** | **Электроника и схемотехника**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями изучения дисциплины являются: ознакомление студентов с законами преобразования и способами передачи информационных сигналов в электронных устройствах и линиях связи; | *Общая трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | формирование знаний в области схемотехники аналого-вых и цифровых электронных устройств<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Электроника и схемотехника входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Алгебра и геометрия<br>Информатика<br>Физика<br>Математический анализ<br>Дискретная математика<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Электроника и схемотехника» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>основы теории электрических цепей; принципы работы элементов и функциональных узлов электронной аппаратуры; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br>Уметь<br>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<br>Владеть<br>навыками работы с программными средствами схемотехнического моделирования; навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма | *составляет **5** зачетных единицы **180** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | работы узла, устройства и системы по комплексу документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы<br>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать Математические методы расчёта электрических цепей, теорию четырёхполюсников, Фурье преобразование и преобразования Лапласса, основы цифровой обработки сигналов<br>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<br>Владеть Навыками проектирования схем аналоговой и цифровой электроники для обработки информации<br>**Дисциплина включает в себя следующие разделы:**<br>1. Электрические цепи, сигналы<br>1.1 Электрические цепи<br>1.2 Цепи при гармоническом воздействии<br>1.3 Методы анализа сложных электрических цепей<br>1.4 Четырехполюсники, фильтры и длинные линии связи<br>1.5 Сигналы и их спектры<br>2. Схемотехника<br>2.1 Полупроводниковые приборы<br>2.2 Электронные усилители и преобразователи сигналов<br>2.3 Нелинейные преобразователи сигналов<br>2.4 Импульсные и цифровые устройства<br>2.5 Цифровая обработка сигналов | |
| **Б1.Б.23** | **Безопасность операционных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины (модуля) «Безопасность операционных систем» являются:<br>1. Знакомство студентов с назначением, разновидностями и основными принципа-ми организации современных операционных систем в объеме, достаточном для понимания задач обеспечения безопасности операционных систем.<br>2. Обучение студентов принципам построения защиты информации в операционных системах (ОС) и методам анализа надежности защиты ОС.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Безопасность операционных систем входит в базовую часть учебного плана образовательной программы. Для | *Общая трудоемкость дисциплины составляет **6** зачетных единицы **216** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/практик: Информатика<br>Безопасность сетей ЭВМ<br>Сети и системы передачи информации<br>Организация ЭВМ и вычислительных систем<br>Основы информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Информационная безопасность распределенных информационных систем<br>Управление информационной безопасностью<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Производственная-преддипломная практика<br>Методы выявления нарушений информационной безопасности<br>Защита информационно-технологических ресурсов автоматизированных систем<br>Защита программного обеспечения<br>Обеспечение информационной безопасности критической информационной инфраструктурой<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Безопасность операционных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа<br>Знать<br>- правила, процедуры, практические приемы для обеспечения информационной безопасности операционных систем<br>- критерии оценки эффективности и надежности средств защиты операционных систем; специализированные средства выявления уязвимостей ОС;<br>Уметь<br>- реализовывать политику учетных записей пользователей операционной системы;<br>- сформировать комплекс мер защиты информации ограниченного | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | доступа для операционной системы;<br>Владеть<br>- навыками формальной постановки задачи обеспечения информационной безопасности операционной системы.<br>- навыками эксплуатации операционных систем и программных систем с учетом требований по защиты информации ограниченного доступа;<br>- навыками использования программно-аппаратных средств обеспечения информационной безопасности<br>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций<br>Знать<br>- иметь представление об основных средствах защиты ОС в составе информационно-технологических ресурсов автоматизированной системы;<br>- критерии защищенности ОС и сети ЭВМ;<br>- критерии оценки эффективности и надежности средств защиты операционных систем;<br>- принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;<br>Уметь<br>использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;<br>- проводить мониторинг угроз безопасности операционных систем<br>- обеспечивать защиту сетевых подключений средствами операционной системы;<br>Владеть<br>- профессиональной терминологией в области информационной безопасности;<br>- навыками работы с конкретными программными и аппаратными продуктами средств телекоммуникаций, удаленного доступа и сетевыми ОС;<br>- навыками конфигурирования встроенных средств защиты информации ОС;<br>- навыками противодействия угрозами типа «недоверенная загрузка (НДЗ) операционной системы» и несанкционированный доступ (НСД) к операционной системе и вычислительной сети;<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>- основные определения и понятия, используемые в теории операционных систем; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - современные подходы к организации и проведению научных исследований с использованием сетевых технологий;<br>- принципы построения и современные технологии, используемые в современных операционных системах, автоматизированных системах и сетях ЭВМ;<br>Уметь<br>- разрабатывать политику учетных записей пользователей ОС;<br>- обосновать выбор решения по обеспечению требуемого уровня защиты ОС (ИС); готовить публикации по результатам выполненных работ;<br>Владеть<br>- навыками использования операционных систем семейств Unix и Windows в системах защиты информации ;<br>- методами и технологиями исследования безопасности операционных систем.<br>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Знать<br>- основы администрирования в операционных системах семейств UNIX и Windows;<br>- средства и службы удаленного управления и администрирования ОС;<br>- модели разделения администрирования операционных систем семейств UNIX и Windows;<br><br>Уметь<br>-выполнять настройку служб терминала;<br>-создавать и выполнять настройку доменов, групп и учетный записей пользователей;<br>-выполнять настройку и удаленное администрирование файлового сервера для ОС семейств UNIX и Windows;<br>Владеть<br>- Навыками удаленного администрирования ОС семейств UNIX и Windows;<br>-Навыками настройки и управления службами терминала;<br>-Навыками использования командной строки для настройки и проведения удаленного администрирования ОС семейств UNIX и Windows<br>**Дисциплина включает в себя следующие разделы**:<br>1. Предмет безопасности операционных систем<br>1.1 Основные понятия и положения защиты информации в информационно-вычислительных системах<br>1.2 Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности операционных систем<br>2. Операционная система с точки зрения специалиста по информационной безопасности<br>2.1 Общая концепция построения ОС, виды ОС.<br>2.2 ОС семейства Unix и Windows. Концепции в обеспечении защиты<br>3. Структурная схема ОС<br>3.1 Центральные элементы ОС – ядро, пользовательская оболочка, файловая подсистема, сетевая под-система<br>3.2 Периферийные подсистемы ОС. Загрузка ОС и ее этапы<br>4. Многозадачные ОС<br>4.1 Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС<br>4.2 Принципы организации межпрограммного взаимодействия<br>5. Сетевая подсистема ОС<br>5.1 Сетевые сервисы ОС<br>5.2 Принципы построения сетевой подсистемы ОС Характерные уязвимости сетевой подсистемы ОС<br>6. Подготовка к промежуточной аттестации(зачет)<br>6.1 Подготовка к промежуточной аттестации<br>7. Подсистема безопасности ОС<br>7.1 Подсистема безопасности ОС. Основные компоненты<br>7.2 Модели безопасности в различных семействах ОС<br>7.3 Дискреционный и мандатный принципы управления доступом – сравнительный анализ<br>8. Администрирование операционных систем<br>8.1 Модели пользователей в различных ОС<br>8.2 Профиль пользователя, бюджет, авторизация, аутентификация пользователя ОС<br>8.3 Назначение прав пользователю ОС и аудит его действий<br>8.4 Аудит системных событий ОС<br>9. Противодействие атакам на информационные системы<br>9.1 Методология атаки и их разновидности<br>9.2 Методы обнаружения и предотвращения атак на информационные системы<br>10. Подготовка к итоговой аттестации<br>10.1 Экзамен | |
| **Б1.Б.24** | **Безопасность сетей ЭВМ**<br>**1 Цели освоения дисциплины (модуля)**<br>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». | *Общая трудоемкость дисциплины составляет* ***7*** |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Специальными целями освоения дисциплины (модуля) «Безопасность сетей ЭВМ» являются:<br>1. Обучение обучающихся организации защиты сетевых устройств и каналов передачи информации, обнаружения и предотвращения несанкционированного доступа к информации в сетях ЭВМ.<br>2. Обучение обучающихся принципам построения систем защиты информации в локальных вычислительных сетях (ЛВС) и методам анализа надежности защиты ЛВС<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Безопасность сетей ЭВМ входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Организация ЭВМ и вычислительных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Информационная безопасность распределенных информационных систем<br>Криптографические методы защиты информации Разработка и эксплуатация защищенных автоматизированных систем<br>Тестирование систем защиты информации автоматизированных систем<br>Защита электронного документооборота<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Виртуальные сети<br>Защита информационно-технологических ресурсов автоматизированных систем<br>Методы проектирования систем защиты распределенных информационных систем<br>Научно-исследовательская работа<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Безопасность сетей ЭВМ» обучающийся должен обладать следующими компетенциями:<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | *зачетных единицы* ***252*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Знать<br>- Характерные уязвимости, присущие каналами связи сетей ЭВМ при передаче информации по ним;<br>- Основные принципы методик противодействия перехвату и несанкционированному съему информации при ее передаче по каналам связи сетей ЭВМ;<br>- Классификацию и основные принципы действия оборудования и ПО, предназначенного для организации защищенных каналов передачи информации.<br>Уметь<br>─ Применять действующую нормативную базу при обеспечении безопасности сетей ЭВМ;<br>─ Определять основные угрозы безопасности в сетях ЭВМ;<br>─ Контролировать безотказное функционирование средств защиты информации в сетях ЭВМ;<br>─ Осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ;<br>─ Разрабатывать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой информации в сетях ЭВМ.<br>Владеть<br>─ Методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ;<br>─ Навыками настройки протоколов безопасности на современном сетевом оборудовании;<br>─ Приемами определения и классификации сетевых атак;<br>─ Методологией составления политик сетевой безопасности.<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>─ Нормативные и правовые акты в области защиты информации передаваемой в сетях ЭВМ;<br>─ Современные технологии обеспечения информационной безопасности в сетях ЭВМ;<br>─ Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в сетях ЭВМ.<br>Уметь<br>- Производить анализ вычислительной сети и сетевого оборудования на предмет наличия известных уязвимостей;<br>- Выполнять подбор необходимого сетевого оборудования, программных и аппаратных средств обеспечения сетевой безопасности;<br>- Выполнять установку и настройку средств защиты информации при эксплуатации их в современной вычислительной сети;<br>- Разрабатывать и реализовать политику сетевой безопасности при | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | настройке и конфигурировании сетевого оборудования.<br>Владеть<br>- Навыками работы с современными программными сканерами сетевых протоколов и сетевых уязвимостей;<br>- Навыками решения задач по поиску неисправностей вычислительных сетей с целью выявления уязвимостей вычислительных сетей и нейтрализации обнаруженных уязвимостей;<br>- Навыками повышения уровня защищенности вычислительных сетей и оптимизации их работы.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Основные понятия безопасности сетей ЭВМ<br>1.1 Безопасность сетей ЭВМ – история вопроса, современное состояние, тенденции<br>1.2 Основные уязвимости сетей ЭВМ и их использование нарушителем<br>1.3 Парольная защита административного и консольного входов на сетевое оборудование<br>1.4 Защита удаленного подключения к сетевому оборудованию<br>2. Модель безопасности для локальной вычислительной сети<br>2.1 Принцип «обороны в глубину» как базовый принцип при организации защиты сети<br>2.2 Сегментирование ЛВС как способ повышения безопасности сети<br>2.3 Мониторинг состояния транспортной подсистемы как средство контроля за состоянием сетевой безопасности<br>3. Обнаружение и нейтрализация сетевых атак<br>3.1 Понятие «сетевой атаки» - история, классификация, современный подход к вопросу<br>3.2 Фазы сетевой атаки<br>3.3 Методики обнаружения сетевых атак<br>3.4 Основные меры противодействия сетевым атакам; системы обнаружения и предотвращения вторжений<br>4. Технологии безопасности локальных вычислительных сетей<br>4.1 Технология виртуальных ЛВС (VLAN)<br>4.2 Технология Port Security<br>4.3 Технология списков контроля доступа (ACL)<br>5. Подготовка к промежуточной аттестации<br>6. Методы контроля сетей ЭВМ<br>6.1 Анализ сетевого трафика<br>6.2 Перехват сетевых сообщений<br>6.3 Использование защищенных протоколов для защиты сетевого трафика<br>7. Безопасность беспроводных сетей<br>7.1 Устройство и разновидности беспроводных сетей | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 7.2 Проблема безопасности в беспроводных сетях<br>8. Защищенные сети<br>8.1 Понятие защищенной сети<br>8.2 Технология виртуальной частной/защищенной сети (VPN). Классификация сетей VPN<br>8.3 Разновидности технологий VPN<br>8.4 Алгоритмы шифрования, применяемые для организации VPN<br>9. Подготовка к итоговой аттестации и курсовой<br>9.2 Подготовка к итоговой аттестации | |
| **Б1.Б.25** | **Безопасность систем баз данных**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Безопасность систем баз данных входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Языки программирования<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Информационные технологии. Базы данных<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Технология построения защищенных распределенных приложений<br>Информационная безопасность распределенных информационных систем<br>Тестирование систем защиты информации автоматизированных систем<br>Защита электронного документооборота<br>Методы мониторинга информационной безопасности АС<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Управление информационной безопасностью<br>Информационная безопасность систем организационного | *Общая трудоемкость дисциплины составляет **6** зачетных единицы **216** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | управления<br>Научно-исследовательская работа<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Безопасность систем баз данных» обучающийся должен обладать следующими компетенциями:<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа<br>Знать<br>Методы формирования требований по защите информации, обрабатываемой в СУБД.<br>Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.<br>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.<br>Организационные меры по защите информации, обрабатываемой в СУБД.<br>Уметь<br>Использовать методы формирования требований по защите информации, обрабатываемой в СУБД.<br>Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, обрабатываемой в СУБД.<br>Организовывать безопасность АРМ, на которых установлена СУБД.<br>Владеть<br>Методами формирования требований по защите информации, обрабатываемой в СУБД.<br>Навыками анализа методов формирования требований по защите информации, обрабатываемой в СУБД.<br>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций<br>Знать<br>Принципы работы баз данных. Основные средства обеспечения безопасности данных.<br>Принципы администрирования баз данных. Средства обеспечения безопасности данных.<br>Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности данных.<br>Уметь<br>Анализировать работоспособность базы данных.<br>Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД.<br>Самостоятельно применять средства обеспечения безопасности данных.<br>Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций.<br>Организовывать безопасность систем баз данных.<br>Владеть<br>Основными средствами обеспечения безопасности данных.<br>Навыками работы с нормативными документами по администрированию баз данных.<br>Средствами обеспечения безопасности данных.<br>Навыками разработки и администрирования базы данных.<br>Навыками организации безопасности систем баз данных.<br>Средствами обеспечения безопасности данных и АИС.<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>Виды аутентификации и принципы, на которых они основаны.<br>Принципы программирования различных видов карт и ключей доступа.<br>Типы атак на системы данных, использующих различные виды аутентификации<br>Уметь<br>Настраивать систему организации и контроля доступа различного вида.<br>Анализировать и находить решения по защите от атак на системы данных, использующих различные виды аутентификации.<br>Устанавливать средства защиты БД.<br>Владеть<br>Навыками настройки и администрирования средств защиты БД.<br>Навыками разработки системы защиты с учетом особенностей защиты информации, обрабатываемой в СУБД.<br>Навыками анализа критериев оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.<br>**Дисциплина включает в себя следующие разделы**<br>1. Общие положения обеспечения безопасности доступа к данным.<br>1.1 Предмет и содержание дисциплины. Обеспечение безопасности доступа к данным.<br>1.2 Задачи защиты информации обеспечения безопасности доступа | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | к данным.<br>2. Обеспечение надежной аутентификации.<br>2.1 Факторы аутентификации.<br>2.2 Аутентификация с использованием OTP-токенов. Аутентификация с помощью биометрических характеристик. Анализ недостатков методов.<br>3. Управление доступом к данным.<br>3.1 СКУД на базе контактных смарт-карт. СКУД на базе бесконтактных RFID смарт-карт. СКУД на базе биометрических систем.<br>3.2 СКУД на базе ключей eToken. СКУД на базе ключей iButton.<br>4. Парольные политики.<br>4.1 Методы парольной аутентификации.<br>4.2 Аутентификация с помощью запоминаемого пароля. Недостатки методов аутентификации с помощью запоминаемого пароля.<br>6. Документирование баз данных с учетом требований по обеспечению информационной безопасности.<br>6.1 Классы безопасности. Требования, предъявляемые к различным классам безопасности.<br>6.2 Требования к документации с учетом класса безопасности.<br>7. Атаки на системы данных.<br>7.1 Атаки на системы данных, в которых используется аутентификация на основе пароля, и способы защиты от них.<br>7.2 Атаки на системы данных, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от них.<br>7.3 SQL-инъекции<br>8. Применение средств криптографической защиты информации (СКЗИ).<br>8.1 Применение средств криптографической защиты информации (СКЗИ), хранящейся в базах данных, от НСД.<br>8.2 Способы и средства криптографической защиты баз данных.<br>9. СКЗИ «Крипто БД».<br>9.1 Состав и совместимость СКЗИ «Крипто БД». Реализуемые алгоритмы криптографического преобразования в СКЗИ «Крипто БД».<br>9.2 Использование «Крипто БД» в облачных средах. Основные принципы работы «Крипто БД».<br>9.3 Анализ угроз и уязвимостей СУБД Oracle | |
| **Б1.Б.26** | **Основы информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Основы информационной безопасности» является понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной | *Общая трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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».<br>Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Основы информационной безопасности входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Физика<br>Информатика<br>Введение в специальность<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Организационное и правовое обеспечение информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Методы и стандарты оценки защищенности компьютерных систем<br>Методы мониторинга информационной безопасности АС<br>Информационная безопасность систем организационного управления<br>Методы проектирования систем защиты распределенных информационных систем<br>Обеспечение информационной безопасности критической информационной инфраструктурой<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Основы информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации.<br>Системы регулирования возникающих общественных отношений в | *составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информационной сферы.<br>Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.<br>Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.<br>Уметь<br>Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.<br>Использовать инфраструктуру единого информационного пространства РФ в личных целях.<br>Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.<br>Владеть<br>Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.<br>Способами использования информационной инфраструктуры в интересах общественного развития.<br>Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.<br>ПК-3 способностью проводить анализ защищенности автоматизированных систем<br>Знать<br>Основы методологии научных исследований.<br>Технические средства контроля эффективности мер защиты информации.<br>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем<br>Классификацию современных компьютерных систем.<br>Современные способы использования компьютерных технологий для проведения исследований.<br>Технические средства контроля эффективности мер защиты информации.<br>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.<br>Уметь<br>Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Анализировать основные узлы и устройства современных автоматизированных систем.<br>Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах.<br>Эффективно использовать современные компьютерные технологии для изучения предмета исследования.<br>Владеть<br>Представлением о возможности использования информационных технологий для решения профессиональных задач.<br>Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности.<br>Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.<br>Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы.<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>Основные информационные технологии, используемые в автоматизированных системах.<br>Сущность и понятие информационной безопасности и характеристику ее составляющих.<br>Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.<br>Уметь<br>Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Принимать участие в исследованиях и анализе современной научно- технической информации по информационной безопасности.<br>Анализировать современную научно-техническую информацию по информационной безопасности.<br>Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе<br>Владеть<br>Основными методами научного познания в области защиты информации.<br>Навыками участия в проведении исследовательских работ по информационной безопасности. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Профессиональной терминологией в области информационной безопасности.<br>Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах<br>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности<br>Знать<br>Основные меры по защите информации в автоматизированных системах.<br>Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.<br>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.<br>Принципы организации работы малых коллективов исполнителей.<br>Уметь<br>Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.<br>Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.<br>Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.<br>Владеть<br>Профессиональной терминологией в области информационной безопасности.<br>Навыками участия в проведении исследовательских работ по информационной безопасности.<br>Методами синтеза структурных и функциональных схем защищенных автоматизированных систем.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Место и роль информационной безопасности в системе национальной безопасности<br>1.1 Сущность и понятие информации. Понятие национальной безопасности. Основы государственной информационной политики<br>1.2 Угрозы национальной безопасности страны во всех сферах деятельности государства все осуществляемые через информационную среду<br>2. Классификация защищаемой информации и угроз информационной<br>2.1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности<br>2.2 Источники и классификация угроз информационной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности для объектов информатизации<br>3. Способы обеспечения информационной безопасности<br>3.1 Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации<br>3.2 Классификация средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации<br>4. Методы формирования требований по защите информации<br>4.1 Анализ существующих методов и средств, применяемых для защиты информации<br>4.2 Разработка предложений по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению их эффективности | |
| **Б1.Б.27** | **Криптографические методы защиты информации**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Криптографические методы защиты информации» является ознакомление обучающихся с основным понятиям 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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Криптографические методы защиты информации входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Введение в специальность<br>Организация ЭВМ и вычислительных систем<br>Теория информации<br>Информатика<br>Языки программирования<br>Теория вероятностей, математическая статистика<br>Математический анализ<br>Основы информационной безопасности<br>Теория графов и ее приложения<br>Математическая логика и теория алгоритмов<br>Исследование операций и теория игр | *Общая трудоемкость дисциплины составляет **7** зачетных единицы **252** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Технологии и методы программирования<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Основы теории оптимизации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Защита электронного документооборота<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Управление информационной безопасностью<br>Защита программного обеспечения<br>Методы проектирования систем защиты распределенных информационных систем<br>Обеспечение информационной безопасности критической информационной инфраструктурой<br>Системы управления информационной безопасностью<br>Информационная безопасность систем организационного управления<br>Научно-исследовательская работа<br>3 Компетенции обучающегося, формируемые в результате освоения<br>дисциплины (модуля) и планируемые результаты обучения<br>В результате освоения дисциплины (модуля) «Криптографические методы защиты информации» обучающийся должен обладать следующими компетенциями:<br>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации<br>Знать<br>• Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации.<br>• методы шифрования, использующие классические симметричные алгоритмы,<br>• методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации,<br>• методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера.<br>• общие принципы действия шифровальной машины Энигма<br>• общие принципы шифрования, используемые в алгоритме симметричного шифрования AES<br>• принципы шифрования информации с помощью биграммного шифра Плейфера | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | • Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.<br>Уметь<br>• исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей<br>• Участвовать в настройке криптографических средств обеспечения информационной безопасности.<br>• Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ.<br>• Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.<br>Владеть<br>• Техникой настройки криптографических средств обеспечения информационной безопасности.<br>• Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем.<br>• Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.<br>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<br>Знать<br>• математический аппарат теории информации, теории алгоритмов<br>• процессы генерации простых чисел для систем ассиметричного шифрования<br>• процессы постановки и верификации ЭЦП<br>• математический аппарат шифра скользящей перестановки<br>• принцип работы сети Фейстеля как базовым преобразованием симметричных блочных криптосистем<br>Уметь<br>• корректно применять при решении профессиональных задач математический аппарат теории алгоритмов, теории информации, в том числе с использованием вычислительной техники<br>• реализовывать методы генерации простых чисел средствами | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | вычислительной техники<br>• проводить дешифрование шифра простой перестановки при помощи метода биграмм<br>Владеть<br>• навыками использованием вычислительной техники для реализации криптографических алгоритмов<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение в криптографию. Основные классы шифров и их свойства<br>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.<br>1.2 Шифры перестановки. Шифры замены. Поточные шифры Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок. Одноалфавитные и многоалфавитные замены.<br>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.<br>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.<br>2. Принципы построения криптографических алгоритмов Реализация криптографических алгоритмов<br>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<br>2.2 Шифры с открытыми ключами Криптосистемы RSA и Эль-Гамаля. Преимущества асимметричных систем шифрования. Криптографические хэш-функции. Характеристики и алгоритмы выработки хэш-функций.<br>2.3 Модели криптографических протоколов Понятие криптографического протокола. Основные примеры, классификация криптографических протоколов. Понятие | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | электронной цифровой подписи. Стандарты ЭЦП.<br>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.<br>2.5 Протоколы установления подлинности. Протоколы управления ключами. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы распределения ключей. | |
| **Б1.Б.28** | **Организация ЭВМ и вычислительных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Организация ЭВМ и вычислительных систем входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Для изучения дисциплины необходимы знания , сформированные в результате изучения информатики, физики общеобразовательной школы (элементарные знание дискретной математики, систем исчисления, базовые представления об электромагнитном взаимодействии).<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Электроника и схемотехника<br>Сети и системы передачи информации<br>Техническая защита информации<br>Безопасность сетей ЭВМ<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно- | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | исследовательской деятельности<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Организация ЭВМ и вычислительных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>─ Основные элементы персонального компьютера и их функциональное назначение, базовые топологии автоматизированных систем;<br>─ Логическую, функциональную и структурную схему персонального компьютера, устройства организующие работу вычислительных систем;<br>─ Логику работы центрального процессора при выполнении вычислений и при передаче данных между ЦП и периферийными устройствами ПК.<br>Уметь<br>─ Определять требуемый перечень компонентов ПК под конкретное техническое задание;<br>─ Определять основные неисправности ПК и подключенных к нем устройств;<br>─ Проектировать одноранговые вычислительные сети.<br>Владеть<br>─ Навыками сборки ПК из отдельных комплектующих;<br>─ Навыками работы с осциллографом;<br>─ Навыками настройки адаптеров сетевых подключений<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>─ принципы построения и функционирования, примеры реализаций современных операционных систем;<br>─ принципы работы элементов и функциональных узлов электронной аппаратуры;<br>─ типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br>Уметь<br>─ применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | и дефрагментации диска);<br>─ работать с современной элементной базой электронной аппаратуры<br>Владеть<br>─ навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;<br>─ навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы<br>**Дисциплина включает в себя следующие разделы:**<br>1. История развития вычислительной техники.<br>1.1 Этапы развития вычислительной техники. Концепция машины с хранимой памятью.Типы структур вычислительных машин и систем.<br>2. Представление информации в вычислительных системах<br>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.<br>2.2 Цифровая и аналоговая формы представления информации. Представление информации электрическими сигналами.<br>3. Архитектура и принципы работы основных логических блоков ЭВМ.<br>3.1 Основы построения ЭВМ. Внутренняя организация процессора. Аппаратная организация системы ввода-вывода информации компьютера. Выявление неисправности системы ввода-вывода информации компьютера<br>4. Организация работы памяти ЭВМ.<br>4.1 Иерархическая структура памяти. Основная память ЭВМ. Оперативное и постоянное запоминающие устройства: назначение и основные характеристики. Виды адресации.<br>5. Внутренние интерфейсы ЭВМ<br>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.<br>5.2 Выявление неисправности ПК. Типовые программные средства сервисного на-значения.<br>6. Операционные системы ЭВМ.<br>6.1 Архитектура современных ОС ЭВМ. Реестр ОС. Драйверы устройств и их роль в организации связи между ядром ОС и устройствами ПК.<br>7. Информационные сети | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 7.1 Локальные, корпоративные, глобальные информационные сети. Модели и структуры информационных систем. Базовые топологии. Сетевые программные и технические средства. | |
| **Б1.Б.29** | **Техническая защита информации**<br>**1 Цели освоения дисциплины (модуля)**<br>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».<br>Дисциплина «Техническая защита информации» рассматривает основные принципы и основные направления технической защиты информации.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Техническая защита информации входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Физика<br>Основы радиотехники<br>Теория информации<br>Основы информационной безопасности<br>Электроника и схемотехника<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Управление информационной безопасностью<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Информационная безопасность распределенных информационных систем<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Техническая защита информации» обучающийся должен обладать следующими компетенциями:<br>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, | *Общая трудоемкость дисциплины составляет **6** зачетных единицы **216** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | криптографических и технических средств защиты информации<br>Знать<br>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации.<br>Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.<br>Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.<br>Уметь<br>Участвовать в настройке технических средств обеспечения информационной безопасности.<br>Самостоятельно настраивать технические средства обеспечения информационной безопасности.<br>Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации.<br>Применять технические средства обеспечения информационной безопасности.<br>Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.<br>Владеть<br>Техникой настройки технических средств обеспечения информационной безопасности.<br>Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем.<br>Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.<br>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации<br>Знать<br>Классификацию технических средств перехвата информации<br>Возможности технических средств перехвата информации<br>Организацию защиты информации от утечки по техническим каналам на объектах информатизации.<br>Уметь<br>Классифицировать технические средства перехвата информации.<br>Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации<br>Выявлять каналы утечки информации | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Проводить контроль эффективности мер по защите информации техническими средствами<br>Владеть<br>Средствами технической защиты информации.<br>Методами технической защиты информации.<br>Навыками проведения проверки защищенности информации и эффективности мер по защите информации<br>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать<br>Физические основы функционирования систем обработки и передачи информации.<br>Основные физические явления и законы, используемые при построении средств защиты информации от утечки по техническим каналам.<br>Технические каналы утечки информации.<br>Уметь<br>Применять соответствующий математический аппарат при проведении расчетов защищенности информации<br>Контролировать безотказное функционирование технических средств защиты информации.<br>Заменять отказавшие технические средства защиты информации.<br>Владеть<br>Навыками работы с нормативными правовыми актами в области технической защиты информации.<br>Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Общие положения защиты информации техническими средствами<br>1.1 Предмет и содержание дисциплины.<br>Физические основы функционирования систем обработки и передачи информации<br>1.2 Задачи защиты информации от утечки по техническим каналам.<br>2. Технические каналы утечки информации<br>2.1 Условия и особенности утечки информации. Структура канала утечки. Виды технических каналов утечки информации<br>2.2 Условия образования каналов утечки. Характеристики каналов утечки информации<br>3. Акустический канал утечки информации<br>3.1 Виды акустических каналов утечки информации. Способы перехвата и средства съема информации по акустическому каналу<br>3.2 Способы и средства защиты от съема информации по акустическому каналу.Системы защиты от утечки информации по | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | акустическому каналу<br>4. Вибрационный канал утечки информации<br>4.1 Виды вибрационных каналов утечки информации. Способы перехвата и средства съема информации по вибрационному каналу<br>4.2 Способы и средства защиты от съема информации по вибрационному каналу.Системы защиты от утечки информации по вибрационному каналу.<br>4.3 Подготовка к зачету<br>5. Электромагнитный канал утечки информации<br>5.1 Виды электромагнитных каналов утечки информации. Способы перехвата и средства съема информации по электромагнитному каналу.<br>5.2 Способы и средства защиты от съема информации по электромагнитному каналу. Системы защиты от утечки информации по электромагнитному каналу<br>6. Оптический канал утечки информации<br>6.1 Виды оптических каналов утечки информации. Способы перехвата и средства съема информации по оптическому каналу<br>6.2 Способы и средства защиты от съема информации по оптическому каналу. Системы защиты от утечки информации по оптическому каналу<br>7. Радиоэлектронный канал утечки информации<br>7.1 Диапазоны частот радиоэлектронного канала. Способы перехвата и средства съема информации по радиоэлектронному каналу<br>7.2 Способы и средства защиты от съема информации по радиоэлектронному каналу. Системы защиты от утечки информации по радиоэлектронному каналу<br>8. Поиск средств несанкционированного съема информации<br>8.1 Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях.<br>8.2 Контроль эффективности мер по защите информации техническими средствами | |
| **Б1.Б.30** | **Сети и системы передачи информации**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины «Сети и системы передачи информации» являются овладение студентами необходимым и достаточным уровнем общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».<br>Специальными целями дисциплины «Сети и системы передачи информации» являются:<br>1. Знакомство обучающихся с назначением, разновидностями и | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144*** |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | основными принципами организации и построения вычислительных сетей в объеме, достаточном для понимания задач обеспечения передачи информации по вычислительным сетям и телекоммуникационным каналам связи.<br>2. Обучение обучающихся принципам передачи информации в вычислительных сетях и телекоммуникационных каналах связи.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Сети и системы передачи информации входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Основы информационной безопасности<br>Организация ЭВМ и вычислительных систем<br>Теория информации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Учебная практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Безопасность сетей ЭВМ<br>Безопасность операционных систем<br>Технология построения защищенных распределенных приложений<br>Информационная безопасность распределенных информационных систем<br>Криптографические методы защиты информации<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Защита электронного документооборота<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности<br>Виртуальные сети<br>Защита информационно-технологических ресурсов автоматизированных систем<br>Производственнаz преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Сети и системы передачи информации» обучающийся должен обладать следующими компетенциями:<br>ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно- | *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>- Виды сетевых топологий;<br>- Принципы передачи информации по телекоммуникационным каналам;<br>- Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;<br>- Классификацию сетевых протоколов.<br>Уметь<br>- Самостоятельно диагностировать неисправности сетей ЭВМ;<br>- Контролировать безотказное функционирование сетей ЭВМ;<br>- Осуществлять подбор инструментальных и программных средств тестирования сетей ЭВМ;<br>- Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.<br>Владеть<br>- Методиками проектирования топологии вычислительных сетей;<br>- Навыками определения и поиска неисправностей в сетях ЭВМ;<br>- Навыками настройки сетевого оборудования.<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>- Принципы построения вычислительных сетей;<br>- Классификацию сетей ЭВМ;<br>- Принципы передачи информации по телекоммуникационным каналам связи;<br>- Классификацию сетевого оборудования;<br>- Принципы функционирования и основные структурные и функциональные элементы различных классов сетевого оборудования;<br>- Семиуровневую эталонную модель взаимодействия открытых систем (модель OSI) с твердым пониманием назначения каждого из уровней модели;<br>- Принципы адресации в вычислительных сетях;<br>- Принципы организации межсетевого взаимодействия и межсетевой передачи информации.<br>Уметь<br>- Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками.<br>Владеть<br>- Профессиональным языком и терминологией предметной области (сети ЭВМ);<br>- Современным сетевым оборудованием и программным | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ).<br>**Дисциплина включает в себя следующие разделы:**<br>1. Основные понятия сетей ЭВМ<br>1.1 Сети ЭВМ – история, функциональное назначение, классификация<br>1.2 Принципы передачи информации по сетям ЭВМ<br>1.3 Классификация сетевого оборудования: назначение, принципы действия, основные базовые характеристики<br>1.4 Сетевые протоколы: назначение, разновидности, характеристики<br>2. Эталонная модель взаимодействия открытых систем<br>2.1 Эталонная модель (модель OSI) как фундаментальный принцип построения современных вычислительных сетей<br>2.2 Структурные уровни модели, принципы организации и функциональное назначение каждого из уровней<br>2.3 Стек протоколов TCP/IP как базовый стек протоколов современных сетей ЭВМ<br>3. Организация вычислительных сетей<br>3.1 Виды сетевых топологий<br>3.2 Классификация сетей – локальные, кампусные, глобальные сети. Сходства и различия<br>3.3 Принципы межсетевого взаимодействия<br>3.4 Организация вычислительных сетей на базе стека протоколов TCP/IP<br>4. Технологии передачи информации по телекоммуникационным каналам связи<br>4.1 Телекоммуникационные каналы связи – назначение и область применения<br>4.2 Принципы передачи информации по телекоммуникационным каналам<br>4.3 Применение телекоммуникационных каналов связи для организации межсетевого взаимодействия<br>5. Методы контроля сетей ЭВМ<br>5.1 Анализ сетевого трафика<br>5.2 Просмотр сетевых сообщений<br>6. Беспроводные сети<br>6.1 Устройство и разновидности беспроводных сетей<br>6.2 Создание защищенной беспроводной сети<br>7. Подготовка к промежуточной аттестации | |
| **Б1.Б.31** | **Организационное и правовое обеспечение информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины «Организационное и правовое | *Общая трудоемкость дисципл* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>Задачи дисциплины:<br>• дать представление о законодательстве РФ в области информации;<br>• ознакомить с системой защиты государственной тайны;<br>• ознакомить с правилами лицензирования и сертификации в области защиты информации;<br>• ознакомить с организационными методами защиты информации;<br>• ознакомить с методами обеспечения информационной безопасности.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Организационное и правовое обеспечение информационной безопасности входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Введение в специальность<br>Основы информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Методы выявления нарушений информационной безопасности<br>Моделирование угроз информационной безопасности<br>Методы мониторинга информационной безопасности АС<br>Защита электронного документооборота<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Управление информационной безопасностью<br>Анализ рисков информационной безопасности<br>Защита программного обеспечения<br>Информационная безопасность систем организационного управления<br>Методы проектирования систем защиты распределенных информационных систем<br>Научно-исследовательская работа | *ины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности<br>Знать<br>-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;<br>-правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>- владения юридической терминологией;<br>-навыками работы с правовыми актами; навыками реализации правовых норм; навыками принятия необходимых мер правового регулирования и (или) защиты интересов субъектов правовых отношений<br>Владеть<br>-навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>-виды тайн, закрепленные в российском законодательстве<br>-правовые основы организации защиты государственной тайны и конфиденциальной информации,<br>-задачи органов защиты государственной тайны и служб защиты информации на предприятиях<br>-основы организационного и правового обеспечения информационной безопасности, | |

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | разрабатывать предложения по совершенствованию системы управления ИБ<br>Владеть<br>методами организации и управления деятельностью служб защиты информации на предприятии<br>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности<br>Знать<br>-организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации<br>-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;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>-анализировать и обобщения информации на стадии принятия и реализации управленческого решения,<br>-пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров<br>Владеть<br>-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований,<br>-методами организации и управления деятельностью служб защиты информации на предприятии<br>-навыками организации и обеспечения режима секретности<br>-навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов<br>**Дисциплина включает в себя следующие разделы**:<br>1. Правовое обеспечение информационной безопасности<br>1.1 Законодательство РФ в области информационной безопасности: Основы законодательства Российской федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты<br>1.2 Правовой режим защиты государственной тайны:<br>Понятие государственной тайны. Государственная тайна как | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | особый вид защищаемой информации. Система защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в РФ.<br>1.3 Лицензирование в области защиты информации:<br>Понятие лицензирования. Нормативные правовые акты РФ, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации.<br>1.4 Сертификация в области защиты информации:<br>Понятие сертификации. Нормативные правовые акты РФ и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации.<br>1.5 Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность.<br>2. Организационное обеспечение информационной безопасности<br>2.1 Понятие организационной защиты информации. Сущность организационных методов защиты информации.<br>2.2 Анализ и оценка угроз информационной безопасности объекта.<br>Методы и способы анализа угроз безопасности информации.<br>Порядок проведения оценки опасности угрозы.<br>2.3 Оценка ущерба:<br>Понятие ущерба. Методы и способы оценки ущерба.<br>2.4 Служба безопасности объекта:<br>Место службы безопасности объекта в общей структуре системы защиты государственной тайны и государственной системы защиты информации. Задачи, решаемые службой безопасности объекта.<br>Структура и состав службы безопасности объекта. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности.<br>2.5 Средства и методы физической защиты объекта:<br>Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового<br>2.6 Организация и обеспечение режима секретности:<br>Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне.<br>Требования к помещениям и хранилищам, в которых ведутся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. | |
| **Б1.Б.32** | **Программно-аппаратные средства обеспечения информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)** | *Общая трудоемкость* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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».<br>Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» рассматривает базовые теоретические понятия, лежащие в основе программно-аппаратной защиты информации.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Программно-аппаратные средства обеспечения информационной безопасности входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Теория информации<br>Информатика<br>Языки программирования<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Информационные технологии. Базы данных<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Информационная безопасность распределенных информационных систем<br>Криптографические методы защиты информации<br>Методы и стандарты оценки защищенности компьютерных систем<br>Организационное и правовое обеспечение информационной безопасности<br>Тестирование систем защиты информации автоматизированных систем<br>Защита электронного документооборота<br>Методы мониторинга информационной безопасности АС<br>Аттестация АИС<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности | *дисциплины составляет **5** зачетных единицы **180** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Управление информационной безопасностью<br>Защита программного обеспечения<br>Информационная безопасность систем организационного управления<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Программно-аппаратные средства обеспечения информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>Классификацию современных программных и программно-аппаратных СЗИ.<br>Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ.<br>Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.<br>Уметь<br>Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий.<br>Основные принципы работы всех подсистем системы ИБ АС.<br>Владеть<br>Навыками работы с подсистемами системы информационной безопасности автоматизированной системы.<br>Навыками администрирования системы ИБ АС.<br>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<br>Знать<br>Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ.<br>Способы контрольных проверок работоспособности и | |

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1.1 Предмет и содержание дисциплины. Принципы работы систем обработки и передачи информации.<br>1.2 Задачи и методы защиты информации программно-аппаратными средствами.<br>2. Задачи и методы защиты информации от НСД.<br>2.1 Применение СЗИ от НСД для организации защищенных компьютерных систем.<br>2.2 Электронные ключи и идентификаторы.<br>3. СЗИ от НСД «СТРАЖ NT».<br>3.1 Механизмы системы защиты СЗИ «СТРАЖ NT». Администрирование СЗИ. Аварийное снятие и восстановление системы защиты.<br>3.2 Редактирование параметров системного аудита. Установка параметров целостности. Назначение грифа. Контроль устройств.<br>4. Обеспечение разграничения и контроля доступа пользователей различными способами.<br>4.1 Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin.<br>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». | |
| **Б1.Б.33** | **Разработка и эксплуатация защищенных автоматизированных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Разработка и эксплуатация защищенных автоматизированных систем входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Основы информационной безопасности<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Организационное и правовое обеспечение информационной безопасности | *Общая трудоемкость дисциплины составляет **7** зачетных единицы **252** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Безопасность сетей ЭВМ<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Информационная безопасность распределенных информационных систем<br>Анализ рисков информационной безопасности<br>Управление информационной безопасностью<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br><br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Разработка и эксплуатация защищенных автоматизированных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем<br>основные принципы построения защищенных распределенных компьютерных систем<br>документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах.<br>современные принципы построения архитектуры ИС.<br>Уметь<br><br>осуществлять анализ несложных процессов проектирования<br>применять государственные стандарты при проектировании автоматизированных систем в защищенном исполнении<br>разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов<br>Владеть<br>приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем<br>приемами разработки проектов нормативных документов, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | регламентирующих работу по защите информации<br>навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем;<br>разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ<br>способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;<br>Уметь<br>осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ<br>применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы<br>применять новые информационные технологии в сфере защиты данных<br>Владеть<br>методами исследования новых образцов программных, технических средств и информационных технологий, применяемых в области информационной безопасности<br>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем<br>Знать<br><br>• уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий;<br>• требования к разработке и производству, проведению испытаний, поддержке безопасности СЗИ для определения уровня доверия<br>• положение о системе сертификации средств защиты информации;<br>• продукцию, которую необходимо сертифицировать;<br>• состав участников системы сертификации и их основные функции;<br>• этапы сертификации;<br>• требования к защищенность информации в автоматизированных системах;<br>• требования к проведению испытаний СЗИ;<br>• порядок проведения сертификационных испытаний.<br>Уметь<br>• составлять техническое задание на выполнение работ по | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | проведению сертификационных испытаний;<br>• составлять акт отбора образца;<br>• подать заявку на сертификацию;<br>• оформить экспертное заключение и проект сертификата соответствия по результатам сертификации.<br>Владеть<br>• навыками проведения испытаний средств защиты информации, а также обеспечения безопасности средств защиты информации в ходе их применения<br>**Дисциплина включает в себя следующие разделы:**<br><br>1. Защищенные автоматизированные системы. Основные понятия и классификация<br>1.1 Классификация АС. Информационные технологии, используемые в АС. Жизненный цикл АС. Современные принципы построения архитектуры АИС.<br>2. Разработка защищенных АС<br>2.1 Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении (АСЗИ). Последовательность и содержание этапов разработки АС. Формирование требований к АСЗИ.<br>2.2 Методы, способы и средства обеспечения отказоустойчивости АСЗИ<br>2.3 Разработка АСЗИ. Выбор мер защиты информации для реализации в АС<br>3. Основы эксплуатации защищенных АС<br>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.<br>3.2 Анализ защищенности АС<br>3.3 Организация технического обслуживания защищённых АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.<br>4. Основы администрирования АС<br>4.1 Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования.<br>5. Безопасность критической информационной инфраструктуры РФ<br>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.<br>5.2 Указ президента №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ». Функции | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | центров ГосСОПКА. Правила эксплуатации центров ГосСОПКА. Построения собственного центра ГосСОПКА.<br>6. Сертификации средств защиты информации автоматизированных систем<br>6.1 Положение о системе сертификации средств защиты информации. Состав участников системы сертификации и их основные функции<br>6.2 Руководящие нормативные и методические документы в системе сертификации средств защиты информации. Сертификация автоматизированных систем, средств вычислительной техники, межсетевых экранов, программного обеспечения.<br>6.3 Требования по безопасности информации. Уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий<br>6.4 Порядок сертификационных испытаний. Подготовка к проведению сертификационных испытаний программного обеспечения в системе сертификации ФСТЭК России | |
| **Б1.Б.34** | **Управление информационной безопасностью**<br>**1 Цели освоения дисциплины (модуля)**<br>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<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Управление информационной безопасностью входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организационное и правовое обеспечение информационной безопасности<br>Основы информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Подготовка к защите и защита выпускной квалификационной работы<br><br>**3 Компетенции обучающегося, формируемые в результате** | *Общая трудоемкость дисциплины составляет **7** зачетных единицы **252** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Управление информационной безопасностью» обучающийся должен обладать следующими компетенциями:<br>ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы<br>Знать<br>- задачи органов защиты государственной тайны и служб защиты информации на предприятиях;<br>- систему организационных мер, направленных на защиту информации ограниченного доступа<br>- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;<br>- основные угрозы безопасности информации и модели нарушителя объекта информатизации;<br>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;<br>- принципы формирования политики ИБ организации;<br>Уметь<br>- разрабатывать модели угроз и модели нарушителя ОИ;<br>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;<br>- разрабатывать предложения по совершенствованию системы управления ИБ АС.<br>Владеть<br>- навыками выявления угроз безопасности информации в АС;<br>- владеть навыками разработки политик безопасности различных уровней.<br>ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- особенности решений по ЗИ в информационных процессах и системах;<br>- определения рисков ИБ применительно к ОИ с заданными характеристиками;<br>- методы и подходы к реализации системы управления безопасностью АИС;<br>- методы анализа процессов для определения актуальных угроз.<br>Уметь<br>- оценивать различные инструменты в области проектирования и управления ИБ; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - разрабатывать политики безопасности информации АС;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.<br>Владеть<br>- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.<br>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- нормативные методические документы ФСТЭК России в области ИБ;<br>- основные угрозы безопасности информации и модели нарушителя в ИС;<br>- стратегии обеспечения ИБ, способы их организации и оптимизации.<br>Уметь<br>- оценивать различные инструменты в области проектирования и управления ИБ;<br>- обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности;<br>- расследовать инциденты ИБ;<br>- разрабатывать предложения по совершенствованию СУИБ АС.<br>Владеть<br>- навыками расчета и управления рисками ИБ;<br>- навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.<br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы<br>Знать<br>- основные угрозы безопасности информации и модели нарушителя в ИС;<br>- основные меры по ЗИ в АС.<br>Уметь<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- расследовать инциденты ИБ.<br>Владеть<br>- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС;<br>- терминологией и процессным подходом построения СУИБ.<br>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности<br>Знать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - основы законодательства Российской Федерации;<br>- нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации;<br>- правовые основы организации защиты государственной тайны и конфиденциальной информации;<br>- меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.<br>Уметь<br>- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей;<br>- предпринимать необходимые меры по восстановлению нарушенных прав.<br>Владеть<br>- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.<br>ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации<br>Знать<br>- основные угрозы безопасности информации и модели нарушителя ОИ;<br>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;<br>- принципы формирования политики информационной безопасности организации.<br>Уметь<br>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- разрабатывать частные политики ИБ АС;<br>- контролировать эффективность принятых мер по реализации частных политик ИБ АС.<br>Владеть<br>- навыками выявления угроз безопасности информации в АС;<br>- владеть навыками разработки политик безопасности различных уровней.<br>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах<br>Знать<br>Ключевые процессы менеджмента ИБ | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Требования нормативно-правовых документов, регламентирующих систему менеджмента информационной безопасности (СМИБ)<br>Уметь<br>Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации<br>Определять цели применения мер и средств контроля и управления для обработки рисков<br>Владеть<br>Навыками выбора необходимых мер и средств контроля и управления ИБ<br>Навыками определения способов измерения результативности выбранных мер управления ИБ<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать<br>Этапы построения и использования СМИБ<br>Семейство стандартов ISO/IEC 27000<br>Уметь<br>Оценивать уровень знаний сотрудников в области ИБ<br>Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ<br>Выявлять возможности улучшения СМИБ<br>Владеть<br>Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ<br>**Дисциплина включает в себя следующие разделы:**<br>1. Создание системы управления информационной безопасностью<br>1.1 Основные принципы создания системы управления информационной безопасностью. Структура системы управления информационной безопасностью<br>1.2 Проектирование систем ИБ. Внедрение ISO 27001/17799.<br>1.3 Административный уровень обеспечения ИБ. Политики среднего и нижнего уровня.<br>1.4 Разработка политик ИБ. Профиль защиты. Разработка профилей защиты и заданий по безопасности<br>1.5 Расследование инцидентов ИБ. Администратор безопасности.<br>1.6 Комплект типовых документов по ИБ.<br>1.7 Технические политики ИБ.<br>2. Обеспечение ИБ организаций банковской системы Российской Федерации<br>2.1 Стандарт Банка России (СТО БР ИББС-1.2). Цикл Деминга для СОИБ. Методика оценки соответствия стандарту Банка России. Программные комплексы оценки соответствия<br>2.2 Стандарт безопасности данных индустрии платежных карт | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | (Payment Card Industry Data Security Standard, PCI DSS). Область применения стандарта PCI DSS. Связь между стандартами PCI DSS и PA-DSS<br>2.3 Процесс проведения аудита на соответствие требованиям PCI DSS. Детализация требований по защите данных платежных карт по PCI DSS.<br>2.4 Детализация требований по строгому контролю доступа по PCI DSS. Детализация требований по построению и поддержанию защищенной сети по PCI DSS. Детализация требований к мониторингу и тестированию.<br>2.5 Программа управления уязвимостями. Поддержание политики информационной безопасности. Модельное представление систем электронных платежей. | |
| **Б1.Б.35** | **Инженерная графика**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины (модуля) «Инженерная графика» являются:<br>- овладение студентами знаниями, умениями и навыками, необходимыми для выполнения и чтения чертежей различного назначения и решения на чертежах инженерно-графических задач;<br>- овладение решением задач геометрического моделирования и применения интерактивных графических систем для выполнения и редактирования изображений и чертежей;<br>- овладение достаточным уровнем общепрофессиональной компетенции в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Инженерная графика входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>школьные курсы черчения, геометрии, информатики.<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Инженерная графика» обучающийся должен обладать следующими компетенциями: | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами<br>Знать<br>- основные определения и понятия инженерной графики;<br>- основные правила выполнения чертежей;<br>- основные положения ЕСКД;<br>- нормативные и руководящие материалы, касающиеся выполняемых типов чертежей<br>Уметь<br>- обсуждать способы эффективного решения задач (2D или 3D построения);<br>- объяснять (выявлять и строить) типичные модели задач, чертежей и 3D моделей;<br>- применять знания чтения и построения чертежей в профессиональной деятельности;<br>- использовать знания чтения и построения чертежей и 3D моделей на междисциплинарном уровне<br>Владеть<br>- практическими навыками использования элементов дисциплины для решения задач на других дисциплинах, на занятиях в аудитории и на производственной практике;<br>- методами использования программных средств для решения практических задач;<br>- основными методами решения задач в области инженерной графики;<br>- возможностью междисциплинарного применения полученных знаний;<br>- основными методами исследования в области инженерной и компьютерной графики, практическими умениями и навыками их использования<br>1. Единая система конструкторской документации.<br>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.<br>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.<br>**Дисциплина включает в себя следующие разделы:**<br>1.3 Тема. ГОСТ 2.702-2011 Правила выполнения электрических схем<br>2. Основы начертательной геометрии.<br>2.1 Тема. Методы проецирования. Комплексный чертеж в трех | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | проекциях. Абсолютные и относительные координаты точки.<br>2.2 Тема. Проекции прямой линии. Положение прямой в пространстве. Взаимное расположение прямых. Конкурирующие точки. Определение натуральной величины отрезка прямой методом прямоугольного треугольника. Проекции прямого угла.<br>2.3 Тема. Плоскость. Элементы определяющие плоскость. Различные случаи положения в пространстве. Взаимное положение и принадлежность точек, прямых, плоскостей. Горизонтали, фронтали в плоскостях уровня, проецирующих и общего положения.<br>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).<br>3. Аксонометрические проекции.<br>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.<br>4. Машиностроительное черчение.<br>4.1 Тема. Резьбовые и сварные соединения. Элементы резьбы. Типы резьб. Изображение и обозначение резьбы.<br>4.2 Тема. Сборочный чертеж, чертеж общего вида. Условности и упрощения при выполнении СЧ. Спецификация. | |
| **Б1.Б.36** | **Информационная безопасность распределенных информационных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>Овладение обучающимися необходимым и достаточным уровнем компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет* ***4*** *зачетных единицы* ***144*** *акад. часов* |

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

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | распределенных ИС.<br>Методы и средства анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.<br>Уметь<br>Разрабатывать частные политики безопасности распределенных ИС.<br>Проводить мониторинг и аудит защищенности информационно-технологических ресурсов распределенных ИС.<br>Руководить разработкой и реализацией частных политики безопасности РИС.<br>Осуществлять мониторинг и аудит безопасности АС.<br>Владеть<br>Методиками анализа политики безопасности РИС.<br>Методиками разработки политики безопасности РИС.<br>Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации защищенных распределенных АС.<br>Методиками руководства разработкой политики безопасности РИС.<br>Методами обеспечения требований по ИБ процессов создания и эксплуатации защищенных РАС.<br>ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами<br>Знать<br>Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации.<br>Способы координирования деятельности подразделений по ЗИ на предприятии, в учреждении, организации.<br>Подходы создания междисциплинарных и инновационных проектов.<br>Уметь<br>Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации.<br>Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации.<br>Принимать участие в междисциплинарных и инновационных проектах.<br>Владеть<br>Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации.<br>Навыками организации и реализации междисциплинарных и инновационных проектов.<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в | |

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

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | проектирование системы защиты информации в распределенных информационных системах<br>3.1 Организация безопасности сетевых подключений распределенных информационных систем.<br>3.2 Сложные распределенные системы-сферы применения<br>3.3 Централизованная и децентрализованная модель организации распределенных информационных систем<br>3.4 Этапы работ по проектированию системы ИБ.<br>3.5 Перечень работы по внедрению системы ЗИ | |
| **Б1.Б.37** | **Методы проектирования систем защиты распределенных информационных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями изучения дисциплины «Методы проектирования систем защиты 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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина «Методы проектирования систем защиты распределенных информационных систем» входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Технология построения защищенных распределенных приложений<br>Математическое моделирование распределенных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты** | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **обучения**<br>В результате освоения дисциплины (модуля) «Методы проектирования систем защиты распределенных информационных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>─ источники и классификацию угроз информационной безопасности;<br>─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>─ основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;<br>Уметь<br>─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;<br>─ классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;<br>Владеть<br>─ навыками разработки и документирования распределенных информационных систем;<br>─ методами формирования требований по защите информации;<br>─ навыками анализа основных узлов и устройств современных автоматизированных систем;<br>─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем<br>ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем<br>Знать<br>─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ современную нормативно-правовую базу создания защищенных распределенных информационных систем;<br>─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей<br>Уметь<br>─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;<br>─ применять современные аппаратные средства защиты | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информационных процессов при аудите распределенных компьютерных систем<br>Владеть<br>─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ навыками разработки комплексной инфраструктуры защищенной информационной системы;<br>─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>─ принципы построения и функционирования, примеры реализаций распределенных систем;<br>─ принципы работы элементов и функциональных узлов электронной аппаратуры;<br>─ концепции построения распределенных информационных систем<br>Уметь<br>─ уметь определять особенности современных программных, технических средств и информационных технологий;<br>─ эксплуатировать современные программные, технические средства и информационные технологии;<br>─ проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы<br>Владеть<br>─ методикой эксплуатации современные программных, технических средств и информационных технологий;<br>─ навыками обеспечения безопасности информации с помощью типовых программных средств;<br>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем<br>Знать<br>─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности;<br>─ 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;<br>Уметь<br>─ применять нормативные правовые акты и нормативные | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | методические документы в области обеспечения информационной безопасности;<br>─ разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;<br>─ разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем<br>Владеть<br>─ 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;<br>─ нормативными требованиями по защите информации;<br>─ навыками организации и обеспечения режима секретности<br>**Дисциплина включает в себя следующие разделы**<br>1. Введение в распределенные системы<br>1.1 Определение распределенной системы. Концепции аппаратных решений. Концепции программных решений. Модель клиент-сервер<br>2. Связь и процессы в распределенных системах<br>2.1 Уровни протоколов. Удаленный вызов процедур. Обращение к удаленным объектам.<br>2.2 Связь по средством сообщений. Связь на основе потоков данных.<br>2.3 Потоки выполнения задач. Пользовательские интерфейсы. Серверы объектов<br>3. Синхронизация компонент в распределённых системах<br>3.1 Синхронизация часов. Логические часы.<br>3.2 Глобальное состояние. Алгоритмы голосования. Взаимное исключение.<br>3.3 Распределенные транзакции<br>4. Непротиворечивость и репликация в распределенных системах<br>4.1 Модели непротиворечивости, ориентированные на данные. Модели непротиворечивости, ориентированные на клиента.<br>4.2 Протоколы распределения. Протоколы реплицируемой записи. Протоколы согласования кэшей.<br>5. Защищенность распределенных систем<br>5.1 Защищенные каналы. Аутентификация. Целостность и конфиденциальность сообщений. Защищенное групповое взаимодействие.<br>5.2 Контроль доступа. Брандмауэры. Защита мобильного кода.<br>5.3 Управление защитой. Управление ключами. Управление<br>6. Экзамен | |
| **Б1.Б.38** | **Технология построения защищенных распределенных** | *Общая* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **приложений**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Технология построения защищенных распределенных приложений входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Технологии и методы программирования<br>Языки программирования<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Информационная безопасность распределенных информационных систем<br>Методы проектирования систем защиты распределенных информационных систем<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Технология построения защищенных распределенных приложений» обучающийся должен обладать следующими компетенциями:<br>ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы<br>Знать | *трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - способы организации обмена данными при помощи технологии RPC;<br>- способы организации обмена данными при помощи технологии RMC;<br>- способы организации обмена данными при помощи очередей;<br>- функционал платформы .Net в части организации обмена данными;<br>- функционал Run-Time Engine;<br>- криптографические протоколы обмена информацией;<br>Уметь<br>- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи на языке C#;<br>- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи в среде разработки LabVIEW;<br>Владеть<br>- навыками оформления программной документации по ЕСПД;<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>- способы организации обмена данными по схеме «peer-to-peer»;<br>- способы организации обмена данными при помощи технологии Socket<br>- базовый синтаксис C#;<br>- базовый функционал LabVIEW;<br>- способы обработки ошибок;<br>-способы организации многопоточности;<br>Уметь<br>- применять язык программирования C# для построения консольных клиент/серверных приложений для однократной передачи данных;<br>- применять язык программирования LabVIEW для построения простейших клиент/серверных приложений для однократной передачи данных;<br>- согласовывать формат передаваемых данных и логику обмена информацией.<br>Владеть<br>- навыками разработки приложений на языке C# с применением многопоточности;<br>- навыками разработки приложений на языке LabVIEW с применением многопоточности;<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | деятельности<br>Знать<br>- варианты интерпретации бинарного потока данных;<br>- структуру пакетов данных транспортного уровнять протокола TCP;<br>Уметь<br>- выполнять анализ данных транспортного уровнять протокола TCP при помощи специализированного программного обеспечения;<br>Владеть<br>-навыками сериализации данных;<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение в распределенные приложения<br>1.1 Понятие распределенного приложения. Определение распределенного приложения. Программные компоненты. Требования к распределенным приложениям. Понятие промежуточной среды.<br>1.2 Программные конструкции языка Python и функции платформы .NET необходимые для реализации простейших сетевых приложений.<br>1.3 Функционал среды разработки LabVIEW и платформы Run-Time Engine необходимый для реализации сетевых приложений.<br>2. Методы организации обмена данными в распределенном приложении<br>2.1 Применение удаленного вызова процедуры. Применение удалённого вызова метода. Применение очередей сообщений. Синхронный и асинхронный обмен данными<br>3. Особенности применения клиент/серверной архитектуры при построении распределенных приложений<br>3.1 Применение многопоточности при построении серверной части распределенного приложения. Реализация на Python и в LabVIEW. Сериализация данных. Кроссплатформенное распределенное программное<br>4. Криптографические протоколы обмена информацией.<br>4.1 Применение SSL и SSH для организации защищенного обмена данными. Разработка приложений использующих SSL и SSH на языке Python и в LabVIEW | |
| **Б1.Б.39** | **Введение в специальность**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Введение в специальность » является ознакомление обучающихся с профессиональной деятельностью в сфере разработки, исследования и эксплуатации систем обеспечения информационной безопасности автоматизированных систем в соответствии с требованиями ФГОС ВО для | *Общая трудоемкость дисциплины составляет **2*** |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Введение в специальность входит в базовую часть учебного плана образовательной программы.<br>Дисциплина «Введение в специальность» входит в базовую часть блока 1 образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения «Информатика и информационно-коммуникационные технологии», «Алгебра» и «Физика» в объеме средней общеобразовательной школы.<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Основы безопасности цифрового общества<br>Основы информационной безопасности<br>Моделирование угроз информационной безопасности<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Введение в специальность» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>• политику государства в области обеспечения информационной безопасности<br>• национальные, межгосударственные и международные стандарты в области защиты информации<br>• современное состояние рынка труда в области обеспечения информационной безопасности | *зачетных единицы* ***72*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | • профессиональный стандарт «Специалист по защите информации в автоматизированных системах»<br>• трудовое законодательство РФ<br>Уметь<br>• анализировать информацию по вопросам национальной и информационной безопасности государства;<br>• соблюдать нормы профессиональной этики<br>Владеть<br>• профессиональной терминологией в области информационной безопасности;<br>• практическими навыками соблюдения норм профессиональной этики.<br>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<br>Знать<br>• Основы построения систем обработки и передачи информации, их современное состояние развития.<br>• Основные задачи обеспечения безопасности информации в компьютерных и автоматизированных системах.<br>• Особенности обработки информации с использованием компьютерных систем<br>Уметь<br>• Осуществлять поиск и систематизировать современную научно-техническую информацию по рассматриваемым вопросам в рамках дисциплины.<br>• Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Владеть<br>• Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.<br>• Навыками осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке<br>**Дисциплина включает в себя следующие разделы**:<br>1. Доктрина информационной безопасности<br>1.1 Общие положения. Основные информационные угрозы и состояние информационной безопасности.<br>1.2 Стратегические цели и основные направления обеспечения информационной безопасности<br>2. Организационная основа системы обеспечения информационной безопасности<br>2.1 Деятельность государственных органов по обеспечению | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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<br>3. Национальные интересы РФ в информационной сфере<br>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<br>3.2 Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, в области обеспечения информационной безопасности<br>4. Способы нарушения информационной безопасности<br>4.1 Классификация способов нарушения информационной безопасности<br>4.2 Способы противодействия нарушению информационной безопасности<br>5. Информационные войны<br>5.1 Классификация и способы информационной войны. Объекты воздействия. Источники угроз. Анализ риска информационной войны<br>6. Криптография и стеганография<br>6.1 Классическая, компьютерная и цифровая стеганография. Атаки на стегосистемы. Применение стеганографии<br>6.2 Криптография и криптоанализ. Криптографические методы. Основные проблемы криптографии. Законодательство в области криптографии и стеганографии.<br>7. Технические каналы утечки информации<br>7.1 Причины утечек данных и возможные ситуации. Классификация технических каналов утечки информации. Использование технических каналов утечки информации<br>7.2 Средства и системы для обнаружения утечки информации. Способы защиты информации | |
| **Б1.Б.40** | **Продвижение научной продукции.**<br>**1 Цели освоения дисциплины (модуля)**<br>- развитие у студентов личностных качеств, а также формирование общекультурных и общепрофессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению | *Общая трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | подготовки 10.05.03 Информационная безопасность автоматизированных систем;<br>- 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;<br>- освоение студентами навыков проведения патентного поиска, оформления патентной документации.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Продвижение научной продукции входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Экономика<br>Правоведение<br>История<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Основы управленческой деятельности<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Продвижение научной продукции» обучающийся должен обладать следующими компетенциями:<br>ОК-8 способностью к самоорганизации и самообразованию<br>Знать<br>- порядок и особенности выполнения научно-исследовательских работ по государственным контрактам;<br>- отличительные признаки инновационной продукции.<br>Уметь<br>- приобретать знания в области продвижения научной продукции;<br>- определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов.<br>Владеть<br>- классификацией научно-технической продукции, | *составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | профессиональным языком в области продвижения научной продукции;<br>- практическими навыками оценки качества для научно-технической продукции, навыками составления конкурсной документации.<br>ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами<br>Знать<br>- средства и методы стимулирования сбыта продукции. Виды охранных документов интеллектуальной собственности;<br>- основные шаги и правила государственной системы регистрации результатов научной деятельности.<br>Уметь<br>- составлять пакет документов для регистрации программы ЭВМ;<br>- составлять пакет документов для регистрации изобретения или полезной модели.<br>Владеть<br>- способами анализа патентной документации и проведения патентного поиска;<br>- способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды.<br>ОК-2 способностью использовать основы экономических знаний в различных сферах деятельности<br>Знать<br>- систему финансирования инновационной деятельности в различных сферах жизнедеятельности;<br>- принципы, формы и методы финансирования научно-технической продукции;<br>- средства и методы стимулирования сбыта продукции.<br>Уметь<br>- анализировать экономическую и научную литературу;<br>- анализировать рынок научно-технической продукции;<br>- рассчитывать экономические показатели структурного подразделения организации;<br>- анализировать существующие и потенциальные запросы потребителей, возможностей создания ценностей для потребителя с учетом особенностей жизненного цикла продукции и технологий;<br>- выделять основные этапы продвижения научного товара и пути его совершенствования в условиях Российского рынка научной продукции;<br>- определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный ресурсов. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>- способами оценивания значимости и практической пригодности инновационной продукции;<br>- методами стимулирования сбыта продукции;<br>- расчетом цен инновационного продукта;<br>- современными методиками расчета и анализа показателей и индикаторов, характеризующие инновационную деятельность предприятия и возможности реализации инновационного проекта.<br>ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности<br>Знать<br>- основные виды охранных документов интеллектуальной собственности;<br>- ключевые этапы и правила государственной системы регистрации результатов научной деятельности;<br>- формы государственной поддержки инновационной деятельности в России.<br>Уметь<br>- анализировать социально-политическую и научную литературу;<br>- оформлять документацию;<br>- использовать основные правовые знания при закреплении основных результатов экспериментальной и исследовательской работы;<br>- составлять пакет документов для регистрации изобретения или полезной модели;<br>- составлять пакет документов для регистрации программы ЭВМ.<br>Владеть<br>- вопросами правового регулирования деятельности предприятия;<br>- знаниями о научно-технической политики России;<br>- навыками составления конкурсной документации.<br>**Дисциплина включает в себя следующие разделы:**<br>1.1 Научно-техническая продукция. Общие сведения. Термины и определения предметной области знаний.<br>1.2 Рынок научно-технической продукции: участники, особенности, коммерческие и некоммерческие способы продвижения результатов научно-исследовательской и инновационной деятельности на рынок.<br>1.3 Анализ рисков при продвижении результатов научно-исследовательской и инновационной деятельности на рынок. Виды рисков и способы управления.<br>1.4 Патентная охрана результатов интеллектуальной деятельности. Патентные исследования. Механизмы передачи прав на объекты интеллектуальной собственности.<br>1.5 Инновации: подходы к определению, классификация и источники возникновения. Факторы, сдерживающие процесс | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | создания инноваций в России.<br>1.6 Инновационный процесс. Основные особенности и этапы инновационного процесса.<br>1.7 Экспертиза инновационных проектов.<br>Понятие и критерии коммерциализуемости инновационного проекта.<br>1.8 Основы бизнес-планирования.<br>1.9 Формы и источники финансирования научно-исследовательской и инновационной деятельности. | |
| **Б1.Б.41** | **Физическая культура и спорт**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Физическая культура и спорт входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Адаптивные курсы по физической культуре и спорту<br>Элективные курсы по физической культуре и спорту<br>Безопасность жизнедеятельности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Элективные курсы по физической культуре и спорту<br>Подготовка к сдаче и сдача государственного экзамена<br>Адаптивные курсы по физической культуре и спорту<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Физическая культура и спорт» обучающийся должен обладать следующими компетенциями:<br>ОК-9 способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности<br>Знать | *Общая трудоемкость дисциплины составляет **2** зачетных единицы **72** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>Уметь<br>Применять полученные теоретические знания по организации и планированию занятий по физической культуре анатомо-физиологических особенностей организма.<br>Применять теоретические знания по организации самостоятельных занятий с учетом собственного уровня физического развития и физической подготовленности.<br>Использовать тесты для определения физической подготовленности с целью организации самостоятельных занятий по определенному виду спорта с оздоровительной направленностью, для подготовки к профессиональной деятельности.<br>Владеть<br>Средствами и методами физического воспитания.<br>Методиками организации и планирования самостоятельных занятий по физической культуре.<br>Методиками организации физкультурных и спортивных занятий с учетом уровня физической подготовленности и профессиональной деятельности, навыками и умениями самоконтроля<br>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<br>Знать<br>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.<br>Уметь<br>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.<br>Владеть<br>Навыками исторического, историко-типологического, сравнительно-типологического анализа для определения места | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>ОПК-7 способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций<br>Знать<br>- основные понятия о приемах первой помощи;<br>- основные понятия о правах и обязанностях граждан по обеспечению безопасности жизнедеятельности;<br>- характеристики опасностей природного, техногенного и социального происхождения;<br>- государственную политику в области подготовки и защиты населения в условиях чрезвычайных ситуаций<br>Уметь<br>- выделять основные опасности среды обитания человека;<br>- оценивать риск их реализации<br>Владеть<br>- основными методами решения задач в области защиты населения в условиях чрезвычайных ситуаций<br>**Дисциплина включает в себя следующие разделы:**<br>Раздел 1 Физическая культура в общекультурной и профессиональной подготовке студентов<br>1.1 Физическая культура личности. Основные понятия и определения в области физической культуры. Компоненты физической культуры, ее социальные функции. Уровни сформированности физической культуры личности<br>2. Раздел 2 Организационные и методические основы физического воспитания<br>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<br>3. Раздел 3 Анатомо-морфологические и физиологические основы жизнедеятельности организма человека при занятиях физической культурой<br>3.1 Организм как единая саморазвивающаяся и саморегулирующаяся биологическая система. Внешняя среда и ее воздействие на организм и жизнедеятельность человека. Функциональная активность человека. Биологические ритмы и | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | работоспособность<br>4. Раздел 4 Основы здорового образа жизни студента<br>4.1 Физическое здоровье и его критерии. Ценностные ориентации молодежи на здоровый образ жизни. Контроль и самоконтроль физического состояния.<br>5.1 Виды спорта. Олимпийские игры. Комплекс ГТО в программе физического воспитания студентов (история, организация работы по совершенствованию физических качеств) | |
| **Б1.Б.42** | **Основы безопасности цифрового общества**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью освоения дисциплины «Основы безопасности цифрового общества» является приобретение компетенций, позволяющих решать человеку поставленные задачи или достигать профессионального результата деятельности в условиях глобальной цифровизации общественных и бизнес-процессов.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Основы безопасности цифрового общества входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Информатика<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Основы Data инжиниринга<br>Основы информационной безопасности<br>Моделирование угроз информационной безопасности<br>Сети и системы передачи информации<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Основы безопасности цифрового общества» обучающийся должен обладать следующими компетенциями:<br>Структурный<br>элемент<br>компетенции<br>Планируемые результаты обучения<br>ОК-5 способностью понимать социальную значимость своей | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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<br>Знать<br>- основные профессиональные задачи специалиста по информационной безопасности;<br>- перечень инструкций для информирование персонала об угрозах безопасности информации и о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации;<br>- основы кибербезопасности;<br>Уметь<br>- критически оценивать информацию, полученную в цифровой среде;<br>- оценить достоверность информации, полученной в цифровой среде;<br>- строить логические умозаключения на основании поступающих информации и данных;<br>Владеть<br>- критическим мышлением для анализа информации в цифровой среде;<br>- основами профессиональной деятельности в сфере цифровой экономики в условиях нарастающих угроз безопасности информации;<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>- основные нормативные правовые акты в области защиты информации;<br>- основные законы о цифровых правах граждан РФ;<br>Уметь<br>- находить нужные источники цифровой информации и цифровые данные;<br>- воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными<br>Владеть<br>- способами эффективного использования полученной цифровой информации для решения профессиональных задач;<br>- управлять цифровой информацией и данными;<br>**Дисциплина включает в себя следующие разделы**:<br>1. Цифровое общество | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1.1.1. Индустрия 4.0: что такое четвертая промышленная революция? Понятие цифровых двойников и цифровых теней.<br>1.1.2. Понятие Интернета вещей (IoT).<br>1.2.1. Цифровые права граждан.<br>1.2.2. Понятия: Security-токен и utility-токен.<br>2. Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики<br>2.1.1. Понятие кибербезопасности. Трансформация понятия информационная безопасность<br>2.1.2. Аналитика международного агентства по кибербезопасности и безопасности инфраструктуры (CISA)<br>2.1.3. Аналитика лаборатории Касперского<br>2.1.4. Кибербезопасность на промышленных объектах<br>2.2 Кибергигиена: правила защиты личных персональных данных<br>2.3 Социальная инженерия. Основные типы социальной инженерии и способы защиты<br>2.4 Федеральный Закон «Об информации, информационных технологиях и защите информации». Понятие организационной защиты информации. | |
| **Б1.Б.43** | **Основы Data инжиниринга**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью изучения дисциплины «Основы Data Engineering» является формирование у обучающихся компетенций в области современных технологий обработки и анализа Big Data в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Основы Data инжиниринга входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Введение в специальность<br>Информатика<br>Теория информации<br>Основы безопасности цифрового общества<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Безопасность систем баз данных<br>Информационные технологии. Базы данных<br>Техническая защита информации<br>Защита электронного документооборота<br>**3 Компетенции обучающегося, формируемые в результате освоения** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Основы Data инжиниринга» обучающийся должен обладать следующими компетенциями:<br>Структурный элемент компетенции<br>Планируемые результаты обучения<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br><br>базовые понятия и терминологию Big Data;<br>возможности инструментальных средств программирования для обработки Big Data;<br>основные алгоритмы и структуры для работы с Big Data;<br>основные понятия распределённых систем.<br><br>Уметь<br><br>применять инструментальные средства программирования для обработки Big Date;<br>выявлять скрытые аномалии в данных<br><br>Владеть<br><br>современными технологиями обслуживания Big Data;<br>алгоритмами и методами для обработки Big Data;<br>инструментальными средствами программирования для обработки Big Data.<br>ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах<br>Знать<br><br>основные направления развития, значение Big Data и их роль в современном обществе;<br>основные возможности ИКТ для поиска Big Data из различных источников информации.<br><br>Уметь<br><br>организовывать поиск Big Data в компьютерных системах, сетях и библиотечных фондах;<br>автоматизировать работу с большими массивами данных, получать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | данные из внешних источников.<br><br>Владеть<br><br>методами поиска, хранения и обработки Big Data из различных источников баз данных, библиотечных фондов;<br>методами представления Big Data с использованием информационных, компьютерных и сетевых технологий.<br><br>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<br>Знать<br><br>особенности обработки информации в сфере Big Data<br><br>Уметь<br><br>обобщать, систематизировать, обеспечивать надежную инфраструктуру полученной научно-технической информации в сфере data инжиниринг.<br><br>Владеть<br><br>методами сбора и обобщения научно-технической информации по теоретическим сведениям, проблемам и задачам, решаемым в курсе "Data Инжиниринг", в т.ч. с использованием литературы на иностранном языке.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Основные понятия курса "основы Data Ingineering". Технологии обработки Big Data. Отличие от традиционной технологии.<br>1.1 Понятие Big Data. Технологии хранения и обработки Big Data. Три определяющих характеристики - основные принципы работы - 4V (volume, velocity, variety, value) с Big Data.<br>2. Системы управления Big data.<br>2.1 Современные технологии обслуживания Big Data. Техники и методики анализа, применимые к Big data.<br>2.2 Программное обеспечение, применяемое для структурирования и анализа Big Data. Консолидация и хранение данных в едином пространстве и единой нормализованной модели<br>3. Роль языков программирования Python и R в аналитике больших данных.<br>3.1 Основные элементы языка Питон. Операции, функции, Преобразование типов данных, строки. Управляющие конструкции | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 3.2 Списки, кортежи, множества. Исключения, словари. ООП – классы, объекты, свойства, методы<br>3.3 Чтение файлов. Файлы с разделителями. Извлечение данных из Web –ресурсов. Использование программных интерфейсов. Импорт модулей. Регулярные выражения<br>3.4 Анализ данных (пакеты scipy, scikit-learn, pandas, numpy). Фильтрование и сортировка, группировка, сложная агрегация<br>3.5 Основы архитектуры хранения и обработки больших данных, виды обработки и масштабирования. Синтаксический анализ записей файла больших размеров с использованием стандартных функций и библиотек. Управление данными, уменьшение размерности.<br>3.6 Feature Engineering - пропущенные значения и дублирование. Запуск скриптов. Парсинг динамических элементов средствами Pyton. Парсинг фото и файлов<br>4. Методы сбора и обработки данных из сети Internet<br>4.1 Основы клиент-серверного взаимодействия. Парсинг API Парсинг HTML. BeautifulSoup, MongoDB<br>5. Организация big data. Реляционные СУБД. СУБД NoSQL. Кластеризация<br>5.1 Подходы к организации big data: реляционных SQL и noSQL. Технология<br>MapReduce Системы управления базами данных MongoDB в Python<br>6. Инструменты для аналитики Big Data. Системы анализа Big Data<br>6.1 Культура сбора и источники данных<br>Предобработка и визуализация данных в pandas<br>Улучшение качества работы с данными<br>6.2 Использование Hadoop MapReduce – платформы программирования и выполнения распределённых MapReduce-вычислений, с использованием большого количества компьютеров (узлов, nodes), образующих кластер.<br>6.3 Основы работы в Hadoop и MapReduce<br>инструментами экосистемы Hadoop: HDFS, Yarn, Hive, Hue, Flume, Cassandra<br>Инструменты класса Data Discovery.<br>Apache Spark.<br>Apache Kafka.<br>6.4 Работа с облачными платформами: AWS, EMR, Azure<br>Продвинутые подходы в MapReduce<br>7. Хранилища данных различных типов. ЦОДы. Витрины данных<br>7.1 Хранилища данных (Data Warehouse). Типы хранилищ. ЦОДы. Защищенность, интеграция, агрегация.<br>Разделение наборов данных, используемых для оперативной обработки, и для решения аналитических задач. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| **Б1.Б.44** | **Иностранный язык в профессиональной деятельности**<br>**1 Цели освоения дисциплины (модуля)**<br>Цели освоения дисциплины «Иностранный язык в профессиональной деятельности»: - повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени обучения;<br>- 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Иностранный язык в профессиональной деятельности входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Для изучения дисциплины «Иностранный язык в профессиональной деятельности» необходимы знания, умения, навыки, сформированные в результате освоения дисциплины «Иностранный язык».<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>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<br>Знать<br>- лексический запас должен составить не менее 3000 лексических единиц с учетом вузовского<br>минимума и потенциального словаря, включая термины профилирующей специальности;<br>- определенные приемы, позволяющие совершать познавательную и коммуникативную деятельность;<br>- структурные типы простого предложения, грамматические формы и конструкции; порядок слов<br>простого предложения;<br>- виды письменных и устных высказываний в различных коммуникативных ситуациях;<br>- разговорные формулы этикета профессионального общения, приемы структурирования научного | *Общая трудоемкость дисциплины составляет* ***4*** *зачетных единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | дискурса.<br>Уметь<br>- понимать аутентичную нормативную монологическую и диалогическую речь носителей иностранного языка;<br>- работать с оригинальной литературой научного характера, сопоставлять и определять/ выбирать пути и способы научного исследования (изучение статей, монографий, рефератов, трактатов, диссертаций);<br>- применять полученные знания для преодоления трудностей при переводе с учетом вида перевода, его целей и условий осуществления.<br>Владеть<br>- подготовленной, а также неподготовленной монологической и диалогической речью в пределах изученного языкового материала и в соответствии с избранной специальностью;<br>- терминологией по специальности, а также дискурсивными, лексико-фразеологическими, грамматическими и стилистическими трудностями в текстах, относящихся к сфере основной профессиональной деятельности;<br>- правильно оперировать языковыми средствами английского языка в ситуациях устного общения;<br>- всеми видами чтения (изучающее, ознакомительное, поисковое и просмотровое);<br>- письмом в пределах изученного материала (250-300 слов).<br>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<br>Знать<br>основные приемы и методы, связанные с поиском, изучением, обобщением и систематизацией научно-технической информации<br>Уметь<br>использовать основные приемы и методы для поиска, изучения, обобщения и систематизации научно-технической информации<br>Владеть<br>основными приемами и методами для поиска, изучения, обобщения и систематизации научно-технической информации<br>**Дисциплина включает в себя следующие разделы**:<br>1. Сфера будущей профессиональной деятельности | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1.1 Развитие умений и навыков письма по теме: «История развития профессии и профессиональной сферы»<br>1.2 Развитие навыков чтения текстов по теме. «Современные технологии и перспективы развития профессии и профессиональной сферы»<br>1.3 Развитие навыков говорения по теме « Мировые ведущие предприятия и компании профессиональной сферы»<br>1.4 Развитие умений и навыков оперирования основными грамматическими явлениями, характерными для профессиональной речи. Категория «Залог»<br>2. Моя будущая карьера.<br>2.1 Развитие умений и навыков чтения, письма по теме «Основные сферы применения моей специальности. Охрана труда и рабочее место специалиста»<br>2.2 Развитие навыков говорения «Профессиональные компетенции будущего специалиста»<br>2.3 Развитие навыков письма по теме «Устройство на работу. Прохождение собеседования. Деловая этика»<br>3. Основы профессиональной коммуникации<br>3.1 Развитие навыков перевода профессиональной лексики, формул, метрических единиц<br>3.2 Развитие навыков чтения и перевода текстов по специальности и деловой корреспонденции.<br>3.3 Развитие навыков письма Аннотирование и реферирование текстов по специальности. | |
| **Б1.Б.ДВ. 01.01** | **Элективные курсы по физической культуре и спорту**<br>**1 Цели освоения дисциплины (модуля)**<br>– формирование физической культуры личности будущего профессионала, востребованного на современном рынке труда;<br>– развитие физических качеств и способностей, совершенствование функциональных возможностей организма, укрепление индивидуального здоровья;<br>– формирование устойчивых мотивов и потребностей в бережном отношении к собственному здоровью, в занятиях физкультурно-оздоровительной и спортивно - оздоровительной деятельностью;<br>– овладение технологиями современных оздоровительных систем физического воспитания, обогащение индивидуального опыта занятий специально-прикладными физическими упражнениями и базовыми видами спорта;<br>– овладение системой профессионально и жизненно значимых практических умений и навыков, обеспечивающих сохранение и укрепление физического и психического здоровья;<br>– освоение системы знаний о занятиях физической | *Общая трудоемкость дисциплины составляет* ***0*** *зачетных единицы* ***328*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | культурой, их роли и значении в формировании здорового образа жизни и социальных ориентаций;<br>– приобретение компетентности в физкультурно-оздоровительной и спортивной деятельности, овладение навыками творческого сотрудничества в коллективных формах занятий физическими упражнениями;<br>– сдача нормативов Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (ГТО).<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Элективные курсы по физической культуре и спорту входит в базовую часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>«Физическая культура» в рамках общего полного среднего образования<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Элективные курсы по физической культуре и спорту» обучающийся должен обладать следующими компетенциями:<br>ОК-9 способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности<br>Знать<br>основные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;<br>формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;<br>знание технических приемов и двигательных действий базовых видов спорта;<br>современные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;<br>основные способы самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | физического развития и физических качеств;<br>технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>Уметь<br>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;<br>выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;<br>использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;<br>использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности;<br>анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;<br>анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств;<br>самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>Владеть<br>практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике;<br>навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;<br>практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;<br>техническими приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности;<br>навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | и производственной деятельностью;<br>основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;<br>навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение<br>1.1 Физическая культура в общекультурной и профессиональной подготовке обучающихся<br>1.2 Основы техники безопасности при выполнении упражнений<br>2. Общефизическая подготовка (комплекс ГТО)<br>2.1 Подготовка к выполнению норматива в беге на 100 м (сек)<br>2.2 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз)<br>2.3 Подготовка к выполнению норматива в бег на 3 км (мин)<br>2.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи-см)<br>2.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см)<br>2.6 Подготовка к выполнению норматива (Плавание на 50 м (мин))<br>3. Учебные занятия по видам спорта<br>3.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>4. Общефизическая подготовка (комплекс ГТО)<br>4.1 Подготовка к выполнению норматива в беге на 100 м (сек)<br>4.2 Подготовка к выполнению норматива в беге на 3 км (мин)<br>4.3 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз)<br>4.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см)<br>4.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см) | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 4.6 Подготовка к выполнению норматива (Бег на лыжах на 5 км (мин)<br>4.7 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м)<br>4.8 Подготовка к выполнению норматива (Плавание на 50 м (мин)<br>5. Учебные занятия по видам спорта<br>5.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>6. Общефизическая подготовка (комплекс ГТО)<br>6.1 Подготовка к выполнению норматива в беге на 100 м (сек)<br>6.2 Подготовка к выполнению норматива в беге на 3 км (мин)<br>6.3 Подготовка к выполнению норматива (Подтягивание из виса на высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз)<br>6.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см)<br>6.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см)<br>6.6 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м)<br>6.7 Подготовка к выполнению норматива (Плавание на 50 м (мин)<br>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)<br>7. Учебные занятия по видам спорта<br>7.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>8. Общефизическая подготовка (комплекс ГТО)<br>8.1 Подготовка к выполнению норматива в беге на 100 м (сек)<br>8.2 Подготовка к выполнению норматива в беге на 3 км (мин)<br>8.3 Подготовка к выполнению норматива (Подтягивание из виса на | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | высокой перекладине (количество раз) или рывок гири 16 кг (кол-во раз)<br>8.4 Подготовка к выполнению норматива (Наклон вперед из положения стоя с прямыми ногами на гимнастической скамье (ниже уровня скамьи, см)<br>8.5 Подготовка к выполнению норматива (Прыжок в длину с разбега (см) или прыжок в длину с места толчком двумя ногами (см)<br>8.7 Подготовка к выполнению норматива (Метание спортивного снаряда весом 700 г (м)<br>8.8 Подготовка к выполнению норматива (Плавание на 50 м (мин)<br>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)<br>9. Учебные занятия по видам спорта<br>9.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>10. Учебные занятия по видам спорта<br>10.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>11. Учебные занятия по видам спорта<br>11.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>12. Учебные занятия по видам спорта<br>12.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале) | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение<br>13. Учебные занятия по видам спорта<br>13.1 Спортивные игры (баскетбол, волейбол, футбол, настольный теннис, бадминтон)<br>Гимнастика<br>Атлетическая гимнастика (занятия в тренажерном зале)<br>Легкая атлетика<br>Пауэрлифтинг и гиревой спорт<br>Специальное медицинское отделение | |
| **Б1.Б.ДВ. 01.02** | **Адаптивные курсы по физической культуре и спорту**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями освоения дисциплины (модуля) «Адаптивные курсы по физической культуре и спорту» являются:<br>формирование физической культуры личности будущего профессионала, востребованного на современном рынке труда;<br>развитие физических качеств и способностей, совершенствование функциональных возможностей организма, укрепление индивидуального здоровья;<br>формирование устойчивых мотивов и потребностей в бережном отношении к собственному здоровью, в занятиях физкультурно-оздоровительной и спортивно- оздоровительной деятельностью;<br>овладение технологиями современных оздоровительных систем физического воспитания, обогащение индивидуального опыта занятий физическими упражнениями с учетом нозологии и показателями здоровья;<br>овладение системой профессионально и жизненно значимых практических умений и навыков, обеспечивающих сохранение и укрепление физического и психического здоровья;<br>освоение системы знаний о занятиях физической культурой, их роли и значении в формировании здорового образа жизни и социальных ориентаций;<br>приобретение компетентности в физкультурно-оздоровительной и спортивной деятельности, овладение навыками творческого сотрудничества в коллективных формах занятий физическими упражнениями;<br>получение знаний и практических навыков самоконтроля при наличии нагрузок различного характера, правил усвоения личной гигиены, рационального режима труда и отдыха;<br>максимально возможное развитие жизнеспособности студента, имеющего устойчивые отклонения в состоянии здоровья, за счет обеспечения оптимального режима функционирования | *Общая трудоемкость дисциплины составляет **0** зачетных единицы **328** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>Программа дисциплины для студентов с ограниченными возможностями здоровья и осо-быми образовательными потребностями предполагает решение комплекса педагогических задач по реализации следующих направлений работы:<br>проведение занятий по физической культуре для студентов с отклонениями в состоянии здоровья, включая инвалидов, с учетом индивидуальных особенностей студен-тов и образовательных потребностей в области физической культуры;<br>разработку индивидуальных программ физической реабилитации в зависимости от нозологии и индивидуальных особенностей студента с ограниченными возможностями здоровья; разработку и реализацию физкультурных образовательно-реабилитационных технологий, обеспечивающих выполнение индивидуальной программы реабилитации;<br>разработку и реализацию методик, направленных на восстановление и развитие функций организма, полностью или частично утраченных студентом после болезни, трав-мы; 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;<br>обеспечение психолого-педагогической помощи студентам с отклонениями в состоянии здоровья, использование на занятиях методик психоэмоциональной разгрузки и саморегуляции, формирование позитивного психоэмоционального настроя;<br>проведение спортивно-массовых мероприятий для лиц с ограниченными возможностями здоровья по различным видам адаптивного спорта, формирование навыков судейства;<br>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;<br>реализацию программ мэйнстриминга в вузе: включение студентов с ограниченными возможностями в совместную со здоровыми студентами физкультурно-рекреационную | |

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | здоровья, умственной и физической работоспособности, физического развития и физических качеств;<br>технику выполнения Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>Уметь<br>использовать межпредметные понятия и универсальные учебные действия (регулятивные, познавательные, коммуникативные) в спортивной, физкультурной, оздоровительной и социальной практике;<br>выполнять физические упражнения разной функционально направленности, использовать их в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;<br>использовать разнообразные формы и виды физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;<br>использовать знания технических приемов и двигательных действий базовых видов спорта в игровой и соревновательной деятельности;<br>анализировать и выделять эффективные технологии укрепления и сохранения здоровья, поддержания работоспособности, профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;<br>анализировать индивидуальные показатели здоровья, умственной и физической работоспособности, физического развития и физических качеств;<br>самостоятельно выполнять и контролировать выполнение Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>Владеть<br>практическими навыками использования регулятивных, познавательных, коммуникативных действий в спортивной, физкультурной, оздоровительной и социальной практике;<br>навыками использования физических упражнений разной функционально направленности в режиме учебной и производственной деятельности с целью профилактики переутомления и сохранения высокой работоспособности;<br>практическими навыками использования разнообразных форм и видов физкультурной деятельности для организации здорового образа жизни, активного отдыха и досуга;<br>техническими приемами и двигательными действиями базовых видов спорта, навыками активного применения их в игровой и соревновательной деятельности;<br>навыками использования современных технологий укрепления и сохранения здоровья, поддержания работоспособности, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | профилактики предупреждения заболеваний, связанных с учебной и производственной деятельностью;<br>основными способами самоконтроля индивидуальных показателей здоровья, умственной и физической работоспособности, физического развития и физических качеств;<br>навыками подготовки к выполнению Всероссийского физкультурно-спортивного комплекса «Готов к труду и обороне» (комплекс ГТО).<br>**Дисциплина включает в себя следующие разделы**:<br>1. Введение<br>1.1 Физическая культура в общекультурной и профессиональной подготовке обучающихся<br>1.2 Основы техники безопасности при выполнении упражнений<br>2. Общефизическая подготовка и лечебная физическая культура<br>2.1 Оздоровительная гимнастика<br>2.2 Атлетическая гимнастика<br>2.3 Скандинавская ходьба<br>2.4 Общеразвивающие упражнения с предметами и без предметов<br>2.5 Фитнес<br>2.6 Подвижные игры<br>3. Учебные занятия по видам спорта<br>3.1 • волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>4. Общефизическая подготовка и лечебная физическая культура<br>4.1 Оздоровительная гимнастика<br>4.2 Атлетическая гимнастика<br>4.3 Скандинавская ходьба<br>4.4 Общеразвивающие упражнения с предметами и без предметов<br>4.5 Фитнес<br>4.6 Подвижные игры<br>5. Учебные занятия по видам спорта<br>5.1 волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 6. Общефизическая подготовка и лечебная физическая культура<br>6.1 Оздоровительная гимнастика<br>6.2 Атлетическая гимнастика<br>6.3 Скандинавская ходьба<br>6.4 Общеразвивающие упражнения с предметами и без предметов<br>6.5 Фитнес<br>6.6 Подвижные игры<br>7. Учебные занятия по видам спорта<br>7.1 волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>8. Общефизическая подготовка и лечебная физическая культура<br>8.1 Оздоровительная гимнастика<br>8.2 Атлетическая гимнастика<br>8.3 Скандинавская ходьба<br>8.4 Общеразвивающие упражнения с предметами и без предметов<br>8.5 Фитнес<br>8.6 Подвижные игры<br>9. Учебные занятия по видам спорта<br>9.1 волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>10. Общефизическая подготовка и лечебная физическая культура<br>10.1 Оздоровительная гимнастика<br>10.2 Атлетическая гимнастика<br>10.3 Скандинавская ходьба<br>10.4 Общеразвивающие упражнения с предметами и без предметов<br>10.5 Фитнес<br>10.6 Подвижные игры<br>11. Учебные занятия по видам спорта<br>11.1 волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | • интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>12. Общефизическая подготовка и лечебная физическая культура<br>12.1 Оздоровительная гимнастика<br>12.2 Атлетическая гимнастика<br>12.3 Скандинавская ходьба<br>12.4 Общеразвивающие упражнения с предметами и без предметов<br>12.5 Фитнес<br>12.6 Подвижные игры<br>13. Учебные занятия по видам спорта<br>13.1 • волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>14. Общефизическая подготовка и лечебная физическая культура<br>14.1 Оздоровительная гимнастика<br>14.2 Атлетическая гимнастика<br>14.3 Скандинавская ходьба<br>14.4 Общеразвивающие упражнения с предметами и без предметов<br>14.5 Фитнес<br>14.6 Подвижные игры<br>15. Учебные занятия по видам спорта<br>15.1 • волейбол<br>• настольный теннис<br>• футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон<br>16. Общефизическая подготовка и лечебная физическая культура<br>16.1 Оздоровительная гимнастика<br>16.2 Атлетическая гимнастика<br>16.3 Скандинавская ходьба<br>16.4 Общеразвивающие упражнения с предметами и без предметов<br>16.5 Фитнес<br>16.6 Подвижные игры<br>17. Учебные занятия по видам спорта<br>17.1 • волейбол<br>• настольный теннис | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | • футбол<br>• баскетбол<br>• дартс<br>• интеллектуальные игры (шашки, шахматы, нарды, уголки)<br>• лыжная подготовка<br>• бадминтон | |
| **Б1.В** | **Вариативная часть** | |
| **Б1.В.ОД** | **Обязательные дисциплины** | |
| **Б1.В.01** | **Информационные технологии. Базы данных.**<br>**1 Цели освоения дисциплины (модуля)**<br>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 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Информационные технологии. Базы данных входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Языки программирования<br>Основы информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Безопасность систем баз данных<br>Технологии и методы программирования<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Технология построения защищенных распределенных приложений<br>Информационная безопасность распределенных информационных систем<br>Криптографические методы защиты информации<br>Тестирование систем защиты информации автоматизированных систем | *Общая трудоемкость дисциплины составляет 6 зачетных единицы* ***216*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Защита электронного документооборота<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Информационные технологии. Базы данных» обучающийся должен обладать следующими компетенциями:<br>Структурный<br>элемент<br>компетенции<br>Планируемые результаты обучения<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>− основные информационные технологии, используемые в автоматизированных системах;<br>- основные программные и технические средства для безопасной работы с базой данных (БД);<br>- новые образцы программных, технических средств для БД;<br>- системы управления базами данных;<br>- способы и алгоритм внедрения и продуктивного использования новых программных, технических средств для БД;<br>Уметь<br>- работать в некоторых интегрированных средах систем управления базой данных (СУБД);<br>- построить схему БД в программных средствах создания БД;<br>- быстро приспособиться к работе в новых интегрированных средах СУБД;<br>Владеть<br>- навыками работы на языке манипулирования БД;<br>- методами оценки правильности проектирования БД;<br>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Знать<br>- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;<br>- основные модели данных, физическую организацию баз данных;<br>- последовательность и содержание этапов проектирования баз данных;<br>Уметь<br>- разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - выделять сущности и связи предметной области;<br>- выполнять запросы к базе данных;<br>- нормализовывать отношения при проектировании реляционной базы данных;<br>- создавать объекты базы данных;<br>Владеть<br>- методиками безопасной работы с БД с помощью современных образцов программных, технических средств;<br>-в полной мере средствами администрирования БД в интегрированных средах СУБД.<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>- методологию и этапы проектирования базы данных;<br>- метод «сущность-связь» для проектирования БД;<br>-методы и подходы создания инфологической модели БД;<br>Уметь<br>-разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;<br>- применять средства обеспечения безопасности баз данных;<br>Владеть<br>- основами проектирования БД;<br>- навыками отображения предметной области на конкретную модель данных;<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение в базы данных.<br>1.1 БД и информационные системы.<br>1.2 Функции СУБД. Типовая организация СУБД. Основные функции СУБД.<br>2. Модели данных.<br>2.1 Понятие модели данных. Виды моделей.<br>2.2 Иерархические системы. Достоинства и недостатки.<br>2.3 Сетевые системы. Достоинства и недостатки.<br>3. Общие понятия реляционного подхода к организации БД.<br>3.1 Базовые понятия реляционных БД. Основные концепции и термины.<br>3.2 Основы реляционной алгебры и реляционного исчисления.<br>3.3 Теоретико-множественные операции реляционной алгебры.<br>4. Проектирование реляционных БД.<br>4.1 Инфологическое моделирование. Методики проектирования.<br>4.2 Проектирование реляционных баз данных с использованием нормализации.<br>4.3 Семантическое моделирование данных. Метод проектирования | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | «Сущность-Связь».<br>4.4 Семантическое моделирование в современных CASE-системах.<br>5. Средства автоматизации проектирования.<br>5.1 Модели автоматизации проектирования. Средства автоматизации проектирования.<br>6. Язык SQL.<br>6.1 Функции, основные возможности. Синтаксис.<br>6.2 Операторы определения и манипулирования схемой БД. Типы SQL-запросов.<br>6.3 Определения ограничений целостности и триггеров.<br>7. Распределенная обработка данных.<br>7.1 Модели архитектуры «клиент-сервер». Управление распределенными данными.<br>7.2 Доступ к базам данных в двухзвенных моделях клиент-сервер.<br>8. Модели транзакций<br>8.1 Понятие транзакции. Две базовые модели транзакций: ANSI и расширенная модель транзакций.<br>9. Разработка БД В MS SQL Server<br>9.1 Язык описания данных DDL<br>9.2 Создание таблиц для хранения данных. Использование команд DML для манипулирования данными.<br>9.3 Применение представлений для просмотра и доступа к данным. Управление доступом к индивидуальным объектам базы данных.<br>9.4 Написание многостолбцовых подзапросов<br>Использование скалярных и коррелированных подзапросов<br>Поддержка регулярных выражений в SQL. | |
| **Б1.В.02** | **Моделирование угроз информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Моделирование угроз информационной безопасности входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Математическое моделирование распределенных систем | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Сети и системы передачи информации<br>Основы информационной безопасности<br>Организация ЭВМ и вычислительных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Анализ рисков информационной безопасности<br>Управление информационной безопасностью<br>Подготовка к защите и защита выпускной квалификационной работы<br>Методы проектирования систем защиты распределенных информационных систем<br>Обеспечение информационной безопасности критической информационной инфраструктурой<br>Системы управления информационной безопасностью<br>Защита информационно-технологических ресурсов автоматизированных систем<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Моделирование угроз информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>средства моделирования угроз информационной безопасности.<br>Уметь<br>применять языки, системы и инструментальные средства программирования для моделирования угроз информационной безопасности.<br>Владеть<br>навыками применения инструментальных средств программирования для моделирования угроз.<br>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Знать<br>основные источники угроз ИБ;<br>классификацию угроз информационной безопасности;<br>Типовую модель угроз информационной безопасности<br>Нормативно-методические документы в области моделирования угроз,<br>способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Уметь<br>Разрабатывать частную модель угроз автоматизированной системы<br>Определять актуальные угрозы для автоматизированной системы;<br>разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.<br>Владеть<br>Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите;<br>Навыками разработки частных моделей угроз<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>нормативные правовые акты в области защиты информации;<br>национальные, межгосударственные и международные стандарты в области защиты информации;<br>руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.<br>Порядок разработки модели угроз<br>Уметь<br>оценивать информационные риски в автоматизированных системах;<br>классифицировать и оценивать угрозы безопасности информации;<br>определять подлежащие защите информационные ресурсы автоматизированных систем;<br>анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации.<br>Владеть<br>методами выявления угроз безопасности информации в автоматизированных системах;<br>методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение<br>1.1 Цели и задачи моделирования угроз ИБ Нормативные и правовые акты в области защиты информации<br>2. Этапы моделирования угроз ИБ<br>2.1 Выявление объектов информационной системы подлежащих защите. Определение источников угроз<br>2.2 Наиболее часто реализуемые угрозы. Выявление способов реализации угроз | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 2.3 Угрозы мобильным устройствам.<br>3. Описание информационной системы<br>3.1 Угрозы за счет реализации ТКУИ<br>3.2 Методики построение дерева угроз<br>3.3 Разработка с учетом реализованных защитных мер.<br>Формирование перечня активов, определение их значимости для компании<br>4. Модель угроз ИСПДн информационной системы персональных данных<br>4.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн.<br>4.2 Классификация угроз безопасности персональных данных по способу реализации<br>5. Основные законы распределения вероятностей для статистического моделирования угроз<br>5.1 Ошибки, возникающие при моделировании угроз. Определение вероятности возникновения отдельных угроз. Программные средства моделирования угроз | |
| **Б1.В.03** | **Методы и стандарты оценки защищенности компьютерных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями изучения дисциплины «Методы и стандарты оценки защищенности компьютерных систем» является формирование у обучающихся понятий о принципах и методах оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности; критериях оценки безопасности информационных технологий; отечественных и международных стандартах оценки защищенности информационных систем; освоение методов качественной и количественных оценок систем информационной безопасности в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Методы и стандарты оценки защищенности компьютерных систем входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Сети и системы передачи информации<br>Безопасность систем баз данных | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Безопасность сетей ЭВМ<br>Тестирование систем защиты информации автоматизированных систем<br>Безопасность операционных систем<br>Теория графов и ее приложения<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Анализ рисков информационной безопасности<br>Защита информационно-технологических ресурсов автоматизированных систем<br>Информационная безопасность систем организационного управления<br>Обеспечение информационной безопасности критической информационной инфраструктурой<br>Научно-исследовательская работа<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Методы и стандарты оценки защищенности компьютерных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>- Стандарты в области оценки защищенности компьютерных систем<br>- Критерии оценки безопасности информационных технологий<br>- Методы оценки защищенности компьютерных систем<br>Уметь<br>- Проводить анализ защищенности компьютерных систем<br>- Выполнять оценку систем информационной безопасности<br>- Составлять диаграммы информационной безопасности<br>Владеть<br>- Методами оценки защищенности компьютерных систем<br>- Методами тестирования защищенности компьютерных систем<br>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 | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | в сфере профессиональной деятельности<br>Знать<br>- современные методы и средства защиты информации в компьютерных системах;<br>- принципы и способы использования существующих средств ЗИ в компьютерных системах;<br>- принципы применения современных методов оценки безопасности компьютерных систем;<br>Уметь<br>- выявлять угрозы и определять их актуальность для современных компьютерных систем;<br>- применять современные методы оценки безопасности компьютерных систем;<br>Владеть<br>- практическими навыками применения методов обеспечения безопасности компьютерных систем;<br>- навыками применения современных методов оценки безопасности компьютерных систем.<br>1. Общие вопросы оценки безопасности компьютерных систем<br>1.1 Стандарт "Критерии определения безопасности компьютерных систем"/ "Оранжевая книга".<br>1.2 Стандарт ISO/IEC 15408 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.<br>1.3 ISO 17799 Практические правила менеджмента информационной безопасности<br>1.4 Российские стандарты и руководящие документы в области оценки защищенности<br>2. Методы оценки систем информационной безопасности<br>2.1 Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников.<br>Построение графа атак<br>2.2 Тестирование систем информационной безопасности<br>2.3 Метод экспертных оценок<br>2.4 Метод информационных потоков .<br>2.5 Оценка показателей защиты информации с применением диаграммы Парето<br>2.6 Метод весовых коэффициентов<br>3. Организация оценки безопасности компьютерных систем<br>3.1 Формирование экспертных систем оценки безопасности компьютерных систем | |
| **Б1.В.04** | **Методы выявления нарушений информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Методы выявления нарушений информационной безопасности» является формирование | *Общая трудоемкость дисципл* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | профессиональных навыков мониторинга и аудита АС и тестирования ИС на выявление нарушений безопасности в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».<br><br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Методы выявления нарушений информационной безопасности входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Теория информации<br>Информатика<br>Языки программирования<br>Теория вероятностей, математическая статистика<br>Математический анализ<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Основы информационной безопасности<br>Дискретная математика<br>Теория графов и ее приложения<br>Исследование операций и теория игр<br>Математическая логика и теория алгоритмов<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Математическое моделирование распределенных систем<br>Безопасность систем баз данных<br>Безопасность сетей ЭВМ<br>Моделирование угроз информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Методы мониторинга информационной безопасности АС<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Управление информационной безопасностью<br>Анализ рисков информационной безопасности<br>Информационная безопасность систем организационного | *ины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | управления<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Методы выявления нарушений информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>Знать<br>─ Средства выявления нарушений информационной безопасности;<br>─ Подходы и методы выявления нарушений информационной безопасности;<br>Уметь<br>─ Принимать участие в анализе результатов систем обнаружения вторжений (СОВ);<br>─ Проводить анализ существующих методов выявления нарушений и определять узкие места;<br>Владеть<br>─ Навыками использования средств анализа информационной безопасности;<br>─ Навыками исследования методов и алгоритмов, используемых в работе систем мониторинга ИБ;<br>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы<br>Знать<br>─ Основные принципы работы системы обнаружения вторжений;<br>─ Основные подсистемы системы обнаружения вторжений;<br>Уметь<br>─ Управлять инцидентами ИБ;<br>─ Администрировать систему выявления нарушений информационной безопасности.<br>Владеть<br>─ Навыками работы с системой выявления нарушений информационной безопасности;<br>─ Навыками работы с подсистемами системы выявления нарушений информационной безопасности;<br>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Знать<br>─ Методы обнаружения вторжений;<br>─ Современные системы обнаружения вторжений (СОВ)<br>─ Методы обнаружения аномалий;<br>Уметь<br>─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.<br>Владеть<br>─ Методами выявления угроз ИБ;<br>─ Методами выявления нарушений ИБ.<br><br>**Дисциплина включает в себя следующие разделы:**<br>1. Подходы и методы выявления нарушений ИБ<br>1.1 Системы и методы обнаружения вторжений. Классификация систем обнаружения вторжений. Недостатки существующих систем обнаружения.<br>1.2 Способы построения «образа» нормального функционирования защищаемой системы. Определение общего показателя аномальности.<br>1.3 Анализ методов обнаружения злоупотреблений. Базы сигнатур атак.<br>1.4 Методы обнаружения аномалий: накопление наиболее характерной статистической информации для каждого параметра оценки; обучение нейронных сетей значениями параметров оценки; событийное представление;<br>1.5 Получение единой оценки состояния защищаемой системы. Статистика Байеса. | |
| **Б1.В.05** | **Анализ рисков информационной безопасности**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>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: | *Общая трудоемкость дисциплины составляет 3 зачетных единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Моделирование угроз информационной безопасности<br>Организационное и правовое обеспечение информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Безопасность операционных систем<br>Техническая защита информации<br>Безопасность Интернета вещей<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>Подготовка к защите и защита выпускной квалификационной работы<br><br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Анализ рисков информационной безопасности» обучающийся должен обладать следующими компетенциями:<br>ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы<br>Знать<br>- методологию анализа рисков информационной безопасности;<br>- методики определения информационно-технологических ресурсов, подлежащих защите;<br>- способы применения анализа рисков информационной безопасности при работе над междисциплинарными проектами;<br>- перечень информационно-технологических ресурсов, подлежащих защите способы применения анализа рисков в информационной безопасности при работе над инновационными проектами.<br>Уметь<br>- применять терминологию анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами;<br>- выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.<br>Владеть<br>- терминологией, используемой при анализе особенностей | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите;<br>- навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.<br>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах<br>Знать<br>- Порядок разработки политик безопасности;<br>- методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;<br>Уметь<br>- оценивать информационные риски в автоматизированных системах;<br>- выполнять анализ рисков информационной безопасности в распределенных информационных системах;<br>- анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.<br>Владеть<br>- методиками проведения анализа рисков информационной безопасности распределенных информационных систем;<br>- методами оценки информационных рисков;<br>- навыками разработки политики информационной безопасности автоматизированных систем.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Методики и технологии управления рисками информационной безопасности и их оценки<br>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.<br>1.2 Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей<br>1.3 Методика оценки рисков информационной организации. Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность<br>1.4 Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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<br>1.6 Современные методы и средства анализа и управление рисками информационных систем. Методика FRAP. Методика OCTAVE. Методика RiskWatch | |
| **Б1.В.06** | **Защита информационно-технологических ресурсов автоматизированных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями изучения дисциплины «Защита информационно-технологических ресурсов автоматизированных систем» является формирование у обучающихся навыков определения информационно-технологических ресурсов автоматизированных систем подлежащих защите; проведения исследований информационно-технологических ресурсов; разработки частной модели угроз и нарушителя информационной безопасности; оценки соответствия защиты информационно-технологических ресурсов автоматизированных систем актуальных стандартам в области защиты информации; формирование рекомендаций по комплексу мер направленных на повышение эффективности существующей системы защиты информации в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Защита информационно-технологических ресурсов автоматизированных систем входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Сети и системы передачи информации<br>Моделирование угроз информационной безопасности<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Безопасность систем баз данных<br>Безопасность сетей ЭВМ<br>Техническая защита информации<br>Тестирование систем защиты информации автоматизированных систем | *трудоемкость дисциплины составляет 4 зачетных единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Методы выявления нарушений информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Методы и стандарты оценки защищенности компьютерных систем<br>Криптографические методы защиты информации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Научно-исследовательская работа<br>Подготовка к сдаче и сдача государственного экзамена<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Защита информационно-технологических ресурсов автоматизированных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-2 способностью создавать и исследовать модели автоматизированных систем<br>Знать<br>- структуру и состав автоматизированных систем управления<br>- информационные и технологические ресурсы автоматизированных систем<br>- способы определения и представления информационных потоков автоматизированных систем<br>Уметь<br>- проводить исследование модели автоматизированной системы<br>- определять и классифицировать информационно-технологические ресурсы АС<br><br>Владеть<br>- навыками анализа информационной инфраструктуры автоматизированной системы;<br>- навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.<br><br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>- нормативные правовые акты, стандарты и руководящие документы в области защиты информации;<br>- порядок разработки модели угроз<br>- виды нарушителей информационной безопасности<br>Уметь<br>- определять подлежащие защите информационно-технологические ресурсы автоматизированных систем;<br>- классифицировать и оценивать угрозы безопасности информации;<br>- оценивать потенциал нарушителя информационной безопасности<br>Владеть<br>- методами выявления угроз безопасности информации в автоматизированных системах;<br>- методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.<br>**Дисциплина включает в себя следующие разделы:**<br><br>1. Аудит информационной безопасности информационно-технологических ресурсов автоматизированных систем<br>1.1 Правовые и методологические основы аудита информационной безопасности.<br>1.2 Виды аудита безопасности. Состав работ по проведению аудита безопасности<br>2. Этапы проведения аудита информационной безопасности<br>2.1 Постановка задач и уточнение состава работ<br>2.2 Сбор данных в соответствии с детальным перечнем работ, определенных в ТЗ на аудит<br>2.3 Анализ собранных данных, оценка рисков<br>2.4 Формирование рекомендаций по совершенствованию комплексной системы обеспечения информационной безопасности<br>2.5 Разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечение информационной безопасности по заданной теме (работа с библиографичес ким материалами, справочниками, каталогами, словарями,<br>2.6 Подготовка и оформление итогового отчета об аудите.<br>3. Промежуточная аттестация<br>3.1 Курсовой проект<br>3.2 Экзамен | |
| **Б1.В.07** | **Безопасность Интернета вещей**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Безопасность Интернета вещей» является формирование профессиональных навыков проектирования | *трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасных IoT-систем в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Безопасность Интернета вещей» рассматривает базовые теоретические понятия, принципы проектирования надежных систем на базе IoT-устройств, средства и способы обеспечения информационной безопасности в IoI-системах.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Безопасность Интернета вещей входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Безопасность сетей ЭВМ<br>Безопасность операционных систем<br>Технологии и методы программирования<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Основы Data инжиниринга<br>Основы безопасности цифрового общества<br>Организация ЭВМ и вычислительных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Информационная безопасность распределенных информационных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Методы выявления нарушений информационной безопасности<br>Тестирование систем защиты информации автоматизированных систем<br>Анализ уязвимостей программного обеспечения<br>Методы мониторинга информационной безопасности АС<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Безопасность Интернета вещей» обучающийся должен обладать следующими компетенциями:<br>Структурный<br>элемент<br>компетенции<br>Планируемые результаты обучения<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной | *составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | деятельности<br>Знать<br>- область применения IoT-систем;<br>- архитектуру IoT-систем;<br>- принципы построения систем на базе IoT-устройств;<br>Уметь<br>- планировать работы по проектированию сложных IoT-систем;<br>- проектировать структуру и архитектуру системы на базе IoT-устройств с использованием современных технологий<br>Владеть<br>- навыками проектирования, тестирования и отладки систем на базе IoT-устройств;<br>ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах<br>Знать<br>- архитектуру безопасности Интернета вещей;<br>- угрозы безопасности IoT-систем;<br>- уязвимости информационных систем, содержащих IoT-устройства<br>Уметь<br>- разрабатывать, руководить разработкой политики безопасности информационных систем, содержащих IoT-устройства;<br>Владеть<br>- навыками проектирования защищенных IoT-систем<br>**Дисциплина включает в себя следующие разделы:**<br><br>1. Проектирование IoT-систем<br>1.1 Принципы построения систем на базе IoT-устройств. Состав IoT систем: сенсоры, актуаторы, гейты<br>1.2 Основные технологии IoT систем. Облачные платформы. Сбор, хранение и обработка данных<br>2. Безопасность IoT-систем<br>2.1 Архитектура безопасности Интернета вещей. Угрозы и уязвимости информационных систем, содержащих IoT-устройства<br>2.2 Оценка рисков в Iot-системах | |
| **Б1.В.08** | **Аттестация АИС**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «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 | *трудоемкость дисциплины составляет **3** зачетных* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | автоматизированных систем». Дисциплина «Аттестация АИС» рассматривает базовые теоретические понятия, средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина «Аттестация АИС» входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Теория информации<br>Информатика<br>Языки программирования<br>Теория вероятностей, математическая статистика<br>Математический анализ<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Основы информационной безопасности<br>Дискретная математика<br>Теория графов и ее приложения<br>Исследование операций и теория игр<br>Математическая логика и теория алгоритмов<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Математическое моделирование распределенных систем<br>Безопасность систем баз данных<br>Безопасность сетей ЭВМ<br>Техническая защита информации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Методы мониторинга информационной безопасности АС<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Управление информационной безопасностью<br>Анализ рисков информационной безопасности<br>Информационная безопасность систем организационного управления<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате** | *единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | **освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Аттестация АИС» обучающийся должен обладать следующими компетенциями:<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>Знать<br>─ Средства анализа информационной безопасности;<br>─ Классификацию систем защиты информации;<br>─ Средства организации аттестации по требованиям безопасности информации.<br>Уметь<br>─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов;<br>─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.<br>Владеть<br>─ Навыками использования средств анализа информационной безопасности;<br>─ Навыками проведения аттестации в соответствии с существующими нормативами.<br>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем<br>Знать<br>─ Источники и классификацию угроз информационной безопасности;<br>─ Основные принципы построения систем защиты информации;<br>─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.<br>Уметь<br>─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.<br>Владеть<br>─ Методами выявления угроз информационной безопасности автоматизированных систем;<br>─ Методами аудита уровня защищенности АИС.<br>**Дисциплина включает в себя следующие разделы**: | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1. Общие положения проведения аттестационных испытаний<br>1.1 Предмет и содержание дисциплины. Методы проверок и испытаний.<br>1.2 Цели и задачи аттестационных испытаний.<br>2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте<br>2.1 Описание и классификация объектов информатизации.<br>2.2 Работы, выполняемые в ходе аттестационных испытаний АС.<br>2.3 Методики проведения аттестации<br>3.1 Методика проведения аттестации информационной системы по требованиям защиты персональных данных. Подготовка отчетной документации.<br>3.2 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.<br>4. Методика аттестационных испытаний выделенных помещений по требованиям безопасности информации<br>4.1 Условия и порядок проведения аттестационных испытаний ВП.<br>4.2 Объемы испытаний на соответствие требованиям по защите информации для ВП. Подготовка отчетной документации.<br>5. Методы выявления нарушений ИБ<br>5.1 Системы и методы обнаружения вторжений<br>5.2 Способы построения «образа» нормального функционирования защищаемой системы. Определение общего показателя аномальности.<br>5.3 Анализ методов обнаружения злоупотреблений. Базы сигнатур атак. | |
| **Б1.В.09** | **Анализ уязвимостей программного обеспечения**<br>**1 Цели освоения дисциплины (модуля)**<br>Общей целью дисциплины «Анализ уязвимостей программного обеспечения» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей 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 уязвимостей программного обеспечения» являются:<br>- изучить контрольно-испытательные и логико-аналитические методы анализа уязвимости программного обеспечения и способы обеспечения надежности программ для контроля их технологической безопасности;<br>- освоить способы оценки эффективности систем защиты программного обеспечения и технологии разработки систем | *трудоемкость дисциплины составляет 4 зачетных единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | программно-технической защиты программного обеспечения.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Анализ уязвимостей программного обеспечения входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Защита электронного документооборота<br>Методы мониторинга информационной безопасности АС<br>Безопасность сетей ЭВМ<br>Технология построения защищенных распределенных приложений<br>Технологии и методы программирования<br>Организация ЭВМ и вычислительных систем<br>Языки программирования<br>Безопасность систем баз данных<br>Тестирование систем защиты информации автоматизированных систем<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Подготовка к сдаче и сдача государственного экзамена<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Анализ уязвимостей программного обеспечения» обучающийся должен обладать следующими компетенциями:<br>ПК-3 способностью проводить анализ защищенности автоматизированных систем<br>Знать<br>- перечень инструментов для проведения анализа уязвимостей программного обеспечения;<br>- базовый функционал инструментов для проведения анализа уязвимостей программного обеспечения;<br>Уметь<br>- применять технические средства для проведения анализа | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | уязвимостей программного обеспечения;<br>Владеть<br>- навыками работы с специализированным программным обеспечением для проведения анализа уязвимостей программного обеспечения<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>Методы, способы, средства, последовательность и содержание этапов разработки программного обеспечения и компонентов безопасности программного обеспечения.<br>Уметь<br>- проводить анализ уязвимостей программного обеспечения;<br>- выполнять реверс инжиниринг программного обеспечения;<br>Владеть<br>- навыками противодействия атакам на программное обеспечение;<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- методы повышения уровня безопасности программного обеспечения;<br>Уметь<br>- выполнять работы по оптимизации схем управления автоматизированной системой;<br>- выявлять компоненты программного обеспечения, не обеспечивающие требуемый уровень информационной безопасности;<br>Владеть<br>- навыками определения возможных векторов атаки на программное обеспечение<br>**Дисциплина включает в себя следующие разделы:**<br><br>1. 1. Контрольно-испытательные и логико-аналитические методы анализа уязвимостей программного обеспечения<br>1.1 Языки формальной спецификации программ. Валидация сценариев требований<br>1.2 Методы анализа структур программ. Верификация и валидация программ. Метод верификации композиции правильных компонентов<br>2. 2. Теоретические и формальные методы доказательства правильности программ и их спецификаций<br>2.1 Проблемы анализа уязвимостей программного обеспечения. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Основные уязвимости программного обеспечения.<br>2.2 Алгоритмические и программные закладки<br>3. 3. Методы и средства анализа уязвимостей программ<br>3.1 Лексический и синтаксический верификационный анализ, семантический анализ программ. Верификация моделей программ методом model checking.<br>3.2 Логика дерева вычислений: формализм для представления свойств живости и безопасности, алгоритмы верификации<br>4. 4. Способы обеспечения надежности программ для контроля их технологической безопасности<br>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.<br>4.2 Методы идентификации программ и их характеристик. Способы оценки подобия целевой и исследуемой программ с точки зрения наличия программных дефектов.<br>5. 5. Анализ средств и этапы преодоления систем защиты программного обеспечения<br>5.1 Методы защиты программ от исследования<br>5.2 Технологии разработки систем программно-технической защиты программного обеспечения. Этапы проектирования и разработки систем программно-технической защиты программного обеспечения.<br>6. 6. Оценка эффективности систем защиты программного обеспечения<br>6.1 Критерии оценки: стойкость к исследованию/взлому; отказоустойчивость (надёжность).<br>6.2 Критерии оценки: независимость от конкретных реализаций операционных систем; совместимость; неудобства для конечного пользователя программного обеспечения; побочные эффекты; стоимость; доброкачественность<br>7. Аттестация<br>7.1 Зачет<br>7.2 Курсовая работа | |
| **Б1.В.10** | **Системы управления информационной безопасностью**<br>**1 Цели освоения дисциплины (модуля)**<br>Целями изучения дисциплины «Системы управления информационной безопасностью» являются: формирование компетенций по созданию части системы менеджмента предприятий/организаций предназначенной для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования информационной безопасности.<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *трудоемкость дисциплины составляет 2 зачетных единицы* ***72*** *акад.* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Дисциплина Системы управления информационной безопасностью входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Введение в специальность<br>Организация ЭВМ и вычислительных систем<br>Основы безопасности цифрового общества<br>Информатика<br>Языки программирования<br>Основы Data инжиниринга<br>Теория вероятностей, математическая статистика<br>Основы информационной безопасности<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Сети и системы передачи информации<br>Правоведение<br>Теория графов и ее приложения<br>Моделирование угроз информационной безопасности<br>Математическая логика и теория алгоритмов<br>Технологии и методы программирования<br>Технология построения защищенных распределенных приложений<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Основы теории оптимизации<br>Математическое моделирование распределенных систем<br>Безопасность сетей ЭВМ<br>Безопасность Интернета вещей<br>Безопасность систем баз данных<br>Техническая защита информации<br>Тестирование систем защиты информации автоматизированных систем<br>Организационное и правовое обеспечение информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Безопасность операционных систем<br>Информационная безопасность распределенных информационных систем<br>Производственная-практика по получению | *часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | профессиональных умений и опыта профессиональной деятельности<br>Методы и стандарты оценки защищенности компьютерных систем<br>Криптографические методы защиты информации<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>Управление информационной безопасностью<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Системы управления информационной безопасностью» обучающийся должен обладать следующими компетенциями:<br>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- нормативные методические документы ФСТЭК России в области ИБ АС;<br>- основные угрозы безопасности информации и модели нарушителя в АС;<br>- способы оптимизации систем управления информационной безопасности (СУИБ).<br>Уметь<br>- анализировать применяемые инструменты в области проектирования и управления ИБ с учетом стоимости и категорирования защищаемых объектов;<br>- обосновывать целесообразность применяемых мер по обеспечению ИБ;<br>- разрабатывать предложения по совершенствованию СУИБ АС.<br>Владеть<br>- навыками расследования инцидентов ИБ;<br>- навыками сбора и анализа исходных данных, проведение обследования бизнес-процессов компании, входящих в область действия СУИБ;<br>- навыками оценки активов (первичных и вторичных) компании, входящих в область действия СУИБ;<br>- навыками определения владельцев и ценности активов; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации<br>Знать<br>- принципы разработки политики информационной безопасности компании/организации;<br>- области действия СУИБ;<br>Уметь<br>- разрабатывать частные Политики ИБ;<br>- определять цели и механизмы контроля обработки рисков ИБ и оценки их применимости для конкретного решения;<br>Владеть<br>- навыками обучение и повышение осведомленности персонала предприятия/организации в области обеспечения безопасности информации;<br>- навыками документирование процессов управления ИБ (политики, процедуры, записи);<br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы<br>Знать<br>- отечественные и международные стандарты по информационной безопасности;<br>- требования в области ИБ для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ)<br>Уметь<br>- разрабатывать техническое задание на проектирование СУИБ с учетом выявленных рисков ИБ<br>- выбирать и анализировать технические решения для СУИБ;<br>Владеть<br>- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям международных стандартов;<br>- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям стандартов и законодательства РФ;<br><br>**Дисциплина включает в себя следующие разделы:**<br>1. Средства обеспечения безопасности корпоративной инфраструктуры<br>1.1 Особенности корпоративной инфраструктуры<br>1.2 Основные средства обеспечения безопасности корпоративной инфраструктуры:<br>Системы обнаружения компьютерных атак. Системы мониторинга | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | корпоративной инфраструктуры.<br>2. Кибербезопасность корпоративной инфраструткуры.<br>2.1 Центры мониторинга инцидентов информационной безопасности. Системы мониторинга и управления ИБ (SIEM). Компоненты центра мониторинга. Системы взаимодействия между компонентами центра мониторинга.<br>2.2 Модели безопасности и передовая практика. Анатомия уязвимостей и бреши в данных. Проблемы безопасности с позиции модели STRIDE. Изучение методов, применяемых хакерами и инсайдерами. Способы проникновения в корпоративную сеть. Технические аспекты проникновения. Организация подключения к внутренним сервисам используя реверсивные техники.<br>2.3 Рамки безопасности. Эшелонированная оборона и 4 периметра.<br>2.4 Особенности работы облачных приложений. Безопасность облачных приложений.<br>3. Зачет | |
| **Б1.В.11** | **Обеспечение информационной безопасности критической информационной инфраструктурой**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью освоения дисциплины "Обеспечение информационной безопасности критической информационной инфраструктуры" является получение компетенций, необходимых для осуществления профессиональной деятельности субъектов критической информационной инфраструктуры (КИИ), ответственных за обеспечение безопасности значимых объектов КИИ.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Обеспечение информационной безопасности критической информационной инфраструктурой входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Введение в специальность<br>Теория информации<br>Основы безопасности цифрового общества<br>Информатика<br>Основы информационной безопасности<br>Сети и системы передачи информации<br>Правоведение<br>Физические основы передачи информации<br>Основы радиотехники<br>Моделирование угроз информационной безопасности<br>Математическая логика и теория алгоритмов | *трудоемкость дисциплины составляет 4 зачетных единицы* ***144*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Технология построения защищенных распределенных приложений<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Безопасность систем баз данных<br>Безопасность сетей ЭВМ<br>Безопасность Интернета вещей<br>Техническая защита информации<br>Тестирование систем защиты информации автоматизированных систем<br>Организационное и правовое обеспечение информационной безопасности<br>Методы выявления нарушений информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Безопасность операционных систем<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Аттестация АИС<br>Методы и стандарты оценки защищенности компьютерных систем<br>Криптографические методы защиты информации<br>Иностранный язык в профессиональной деятельности<br>Анализ уязвимостей программного обеспечения<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Производственная-преддипломная практика<br>Управление информационной безопасностью<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Обеспечение информационной безопасности критической информационной инфраструктурой» обучающийся должен обладать следующими компетенциями:<br>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Знать<br>- нормативные и правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - основы функционирования ГосСОПКА;<br>- понятия объектов и субъектов КИИ;<br>Уметь<br>- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;<br>- способы реализации угроз безопасности и возможные последствия от их реализации;<br>- определять требования по устранению возможных уязвимостей, приводящих к возникновению угроз безопасности информации;<br>Владеть<br>- навыками работы с нормативными и правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых объектов КИИ;<br>- навыками работы с информационными базами данных, содержащими информацию по угрозам безопасности информации и уязвимостями ПО значимых объектов КИИ;<br>- навыками выявления и анализа угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей значимого объекта КИИ;<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ;<br>- общие требования по обеспечения безопасности значимых объектов КИИ;<br>- подходы категорирования значимости объектов КИИ;<br>Уметь<br>- определять категории значимых объектов КИИ и оформлять полученные результаты;<br>- определять структуру системы безопасности значимого объекта КИИ;<br>- определят требования по обеспечения безопасности значимых объектов КИИ;<br>- определять требования к параметрам настройки программных и программно-аппаратных средств защиты информации (СЗИ);<br>Владеть<br>- навыками установки и настройки СЗИ, обрабатываемой объектами КИИ;<br>- навыками подбора средств СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;<br>ПК-25 способностью обеспечить эффективное применение средств | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций<br>Знать<br>-требования к организационным и техническим мерам для обеспечения безопасности значимых объектов КИИ;<br>- основные принципы организации государственного контроля состояния защищенности значимых объектов КИИ;<br>- процедуру категорирования объектов КИИ;<br>- требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования;<br>Уметь<br>- осуществлять выбор СЗИ с учетом совместимости с применяемым на значимом объекте КИИ ПО и категорированием значимого объекта КИИ;<br>- определять СЗИ для реализации технических мер обеспечения безопасности информации в рамках системы безопасности значимого объекта КИИ;<br>Владеть<br>- навыками участия в разработке организационных и технических мероприятий по защите объектов КИИ;<br>- навыками разработки организационно-распорядительными документов по безопасности значимых объектов КИИ;<br>- навыками проведения работ по контролю состояния безопасности объектов КИИ;<br><br>**Дисциплина включает в себя следующие разделы:**<br>1. Правовые основы обеспечение безопасности информации объектов КИИ РФ<br>1.1 Понятия объекта и субъекта КИИ.<br>1.2 Законодательство РФ по обеспечение безопасности информации объектов КИИ. Нормативные методические документы ФСТЭК России по обеспечение безопасности информации объектов КИИ.<br>1.3 Угрозы безопасности информации, обрабатываемой на объектах КИИ<br>1.4 Категорирование объектов КИИ<br>1.5 Организация работ по обеспечению безопасности объектов КИИ<br>1.6 ГосСОПКА<br>2. Обеспечение безопасности информации значимых объектов КИИ<br>2.1 Требования по обеспечению безопасности значимых объектов КИИ<br>2.2 Система безопасности значимого объекта КИИ. Этапы разработки<br>2.3 Контроль за обеспечением безопасности значимого объекта | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | КИИ.<br>2.4 Основные программно-технические подсистемы СОБИ КСИИ<br>2.5 Управление ОБИ КСИИ документирование и реализация основных процессов.<br>2.6 Этапы разработки СОБИ КИИ. Аналитическое обоснование необходимости создания СОБИ КИИ.<br>2.7 Техническое задание на разработку СОБИ КИИ. Основные проектные документы. Разработка комплекса внутренних организационно-распорядительных документов | |
| **Б1.В.ДВ.001** | **Дисциплины по выбору Б1.В.ДВ.01** | |
| **Б1.В.ДВ.01.01** | **Основы радиотехники**<br>**1. Цели освоении дисциплины**<br>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 телевещании, радиолокации, радионавигации и радиоподавления, а также разработки программно-аппаратных компонентов защищенных автоматизированных систем.<br>Эта цель достигаются в ходе выполнения следующих задач:<br>– изучение основ излучения, распространения и приема радиоволн;<br>– изучения передающих и приемных антенн различных диапазонов длин волн;<br>– изучение методов формирования и преобразования сигналов;<br>– изучение принципов построения передающей и приемной аппаратуры;<br>– изучение структурных схем и особенностей работы телевизионных радиосистем;<br>– изучение принципов построения отдельных устройств радиотехнических систем приема и передачи информации.<br>**2. Место дисциплины в структуре образовательной программы подготовки специалиста**<br>Дисциплина входит в вариативную часть образовательного стандарта.<br>Для изучения дисциплины необходимы знания (умения, владения) сформированные в результате изучения дисциплин:<br>«Физика»,<br>«Математический анализ»,<br>«Информатика», | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | «Электроника и схемотехника».<br>Дисциплина является необходимой в изучении последующих дисциплин:<br>«Техническая защита информации»,<br>«Программно-аппаратные средства обеспечения информационной безопасности»,<br>«Разработка и эксплуатация защищенных автоматизированных систем».<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины «Основы радиотехники» обучающийся должен обладать следующими компетенциями:<br>**ОПК-1** способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать<br>− физическую сущность процессов, происходящих в системах передачи информации в целом;<br>− физическую сущность процессов, происходящих в отдельных узлах систем передачи информации;<br>− физическую сущность процессов, происходящих в элементах узлов систем передачи информации.<br>Уметь:<br>− разрабатывать модели процессов, происходящих в системах передачи информации в целом;<br>− разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации;<br>− разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.<br>Владеть:<br>− математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом;<br>− математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации;<br>− математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.<br>**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<br>Знать<br>− характеристики и область применимости базовых электронных компонентов; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | − схемотехнику основных электронных узлов радиотехнических систем;<br>− программное обеспечение для разработки систем передачи информации в целом и отдельных её узлов.<br>Уметь:<br>− создавать имитационные модели радиотехнических систем передачи информации с помощью специализированного программного обеспечения;<br>− проводить анализ систем передачи информации в целом;<br>− разрабатывать системы передачи информации в целом и отдельных её узлов;<br>− создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.<br>Владеть:<br>− навыками проектирования и создания отдельных элементов и узлов радиотехнических устройств;<br>− методами анализа работоспособности электронных узлов радиотехнических устройств с помощью специализированного программного обеспечения;<br>− методами разработки системы передачи информации в целом и отдельных её узлов<br>**Дисциплина включает в себя следующие разделы**:<br>**1. Основы построения радиотехнических устройств приема и передачи информации**<br>1.1. Основные понятия, термины и определения<br>1.2. Классификация и структура построения радиотехнических систем связи и вещания.<br>1.3. Диапазоны частот и сигналы.<br>1.4. Особенности распространения радиоволн различных диапазонов.<br>1.5. Построение радиотехнических систем.<br>1.6. Антенно-фидерные устройства.<br>1.7. Радиоприемные устройства.<br>1.8. Радиопередающие устройства.<br>**2. Преобразование информационных сигналов в радиотехнических системах и коммуникационных сетях**<br>2.1. Сигналы, передаваемые в системах радиосвязи и телевидения.<br>2.2. Виды представления сигналов.<br>2.3. Спектры периодических колебаний<br>2.4. Спектры непериодических колебаний.<br>2.6. Виды сообщений и их характеристики. Информация, сообщения, сигналы.<br>2.7. Принцип передачи информации. Виды сигналов<br>2.8. Принципы преобразования аналоговых сообщений | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 2.9. Международные стандарты аналого-цифрового преобразования и сжатия аудио и визуальной информации.<br>**3. Радиотехнические способы защиты информации**<br>3.1. Телекоммуникационные системы электросвязи<br>3.2. Архитектура и принципы построения сетей<br>3.3. Каналы связей и их математические модели<br>3.4. Многоканальные телекоммуникационные системы<br>3.5. Цифровые телекоммуникационные сети<br>3.6. Распределение информации в телекоммуникационных сетях<br>3.7. Интеграция и конвергенция цифровых телекоммуникационных сетей | |
| **Б1.В.ДВ.01.02** | **Физические основы передачи информации**<br>**1. Цели освоении дисциплины**<br>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.<br>Эта цель достигаются в ходе выполнения следующих задач:<br>– изучение физических сред передачи данных, типов линий связи и их характеристик;<br>– изучение основ излучения, распространения и приема радиоволн;<br>– изучение методов формирования и преобразования сигналов;<br>– изучение принципов построения систем передачи информации;<br>– изучение структурных схем и особенностей работы систем многоканальной связи;<br>– изучение принципов построения отдельных устройств систем приема и передачи информации.<br>**2. Место дисциплины в структуре образовательной программы подготовки специалиста**<br>Дисциплина входит в вариативную часть образовательного стандарта.<br>Для изучения дисциплины необходимы знания (умения, владения) сформированные в результате изучения дисциплин:<br>«Физика»,<br>«Математический анализ»,<br>«Информатика»,<br>«Электроника и схемотехника».<br>Дисциплина является необходимой в изучении последующих дисциплин: | *Общая трудоемкость дисциплины составляет 3 зачетных единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | «Техническая защита информации»,<br>«Программно-аппаратные средства обеспечения информационной безопасности»,<br>«Разработка и эксплуатация защищенных автоматизированных систем».<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины «Основы радиотехники» обучающийся должен обладать следующими компетенциями:<br>**ОПК-1** способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать<br>− физическую сущность процессов, происходящих в системах передачи информации в целом;<br>− физическую сущность процессов, происходящих в отдельных узлах систем передачи информации;<br>− физическую сущность процессов, происходящих в элементах узлов систем передачи информации.<br>Уметь:<br>− разрабатывать модели процессов, происходящих в системах передачи информации в целом;<br>− разрабатывать модели процессов, происходящих в отдельных узлах систем передачи информации;<br>− разрабатывать модели процессов, происходящих в элементах узлов систем передачи информации.<br>Владеть:<br>− математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом;<br>− математическим аппаратом для описания процессов, происходящих в отдельных узлах систем передачи информации;<br>− математическим аппаратом для описания процессов, происходящих в элементах узлов систем передачи информации.<br>**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<br>Знать<br>− характеристики и область применимости базовых электронных компонентов;<br>− схемотехнику основных электронных узлов систем передачи информации;<br>− программное обеспечение для разработки систем передачи | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информации в целом и отдельных её узлов.<br>Уметь:<br>− создавать имитационные модели систем передачи информации с помощью специализированного программного обеспечения;<br>− проводить анализ систем передачи информации в целом;<br>− разрабатывать системы передачи информации в целом и отдельных её узлов;<br>− создавать программное обеспечение для разработки системы передачи информации в целом и отдельных её узлов.<br>Владеть:<br>− навыками проектирования и создания отдельных элементов и узлов устройств связи;<br>− методами анализа работоспособности электронных узлов устройств связи с помощью специализированного программного обеспечения;<br>− методами разработки системы передачи информации в целом и отдельных её узлов<br>**Дисциплина включает в себя следующие разделы:**<br>**Системы связи и способы передачи информации**<br>1.1. Сообщения и сигналы.<br>1.2. Системы связи. Канал связи. Помехи и искажения в канале.<br>1.3. Кодирование и модуляция. Демодуляция и декодирование.<br>1.4. Дискретизация и кодирование непрерывных сообщений.<br>1.5. Основные характеристики систем связи.<br>**2. Сообщения, сигналы, помехи**<br>2.1. Сообщения, сигналы и помехи как случайные процессы. Спектры случайных процессов.<br>2.2. Математические способы представления сигналов.<br>2.3. Теорема Котельникова.<br>2.4. Информационные параметры сообщений и сигналов<br>**3. Каналы связи и их характеристики**<br>3.1. Общие сведения о каналах связи.<br>3.2. Прохождение сигналов через каналы с детерминированными характеристиками.<br>3.3. Математические модели каналов связи.<br>3.4. Пропускная способность канала связи.<br>3.5. Теорема кодирования для канала с помехами.<br>**4. Передача дискретных сообщений в непрерывных каналах**<br>4.1. Прием сигнала как статистическая задача. Критерии качества приема дискретных сообщений.<br>4.2. Оптимальные алгоритмы приема при полностью известных сигналах и при сигналах с неопределенной фазой.<br>**5. Основы теории кодирования**<br>5.1. Назначение и классификация кодов. Принципы помехоустойчивого кодирования | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 5.2. Линейные двоичные болчные коды. Разновидности систематических кодов<br>5.3. Эквивалентная вероятность ошибки. Системы с обратной связью.<br>**6. Теория передачи непрерывных сообщений**<br>6.1. Источник непрерывных сообщений и его производительность. Верность передачи непрерывных сообщений.<br>6.2. Оптимальный прием непрерывных сообщений.<br>6.3. Помехоустойчивость систем аналоговой передачи при слабых помехах. Порог помехоустойчивости. Помехоустойчивость систем с импульсной модуляцией.<br>**6. Цифровые методы передачи непрерывных сообщений**<br>6.1. Общие сведения о цифровой передаче непрерывных сообщений.<br>6.2. Помехоустойчивость импульсно-кодовой модуляции. Кодирование с предсказанием.<br>6.3. Эффективность систем связи.<br>**7. Теория многоканальной передачи сообщений**<br>7.1. Основы теории разделения сигналов.<br>7.2. Частотное, временное и фазовое разделение сигналов. Разделение сигналов по форме.<br>7.3. Способы разделения сигналов в асинхронных адресных системах связи | |
| **Б1.В.ДВ.02** | **Дисциплины по выбору Б1.В.ДВ.02** | |
| **Б1.В.ДВ.02.01** | **Основы теории оптимизации**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью дисциплины «Основы теории оптимизации» является 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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Основы теории оптимизации входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Дискретная математика<br>Математический анализ<br>Теория вероятностей, математическая статистика<br>Алгебра и геометрия | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Теория информации<br>Языки программирования<br>Информатика<br>Математическая логика и теория алгоритмов<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Криптографические методы защиты информации<br>Тестирование систем защиты информации автоматизированных систем<br>Моделирование угроз информационной безопасности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Основы теории оптимизации» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>– Общие положения теории оптимизации;<br>– Логическую, функциональную и структурную схему персонального компьютера, устройства организующие работу вычислительных систем;<br>– Способы применения теоретических положений и методов теории оптимизации для постановки и решении профессиональных задач.<br>Уметь<br>– Проводить теоретические исследования применения общих положений и методов теории оптимизации;<br>– Определять возможности применения теоретических положений и методов теории оптимизации для постановки и решения конкретных прикладных задач;<br>– Эффективно использовать и оптимизировать свою работу за счет применения общих положений и методов теории оптимизации<br>Владеть<br>– Приемами использования соответствующего математического аппарата при решении профессиональных задач;<br>– Приемами сбора и анализ исходных данных для последующей | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | обработки соответствующим математическим аппаратом;<br>– Навыками повышения эффективности работы за счет применения общих положений и методов теории оптимизации.<br>ПК-2 способностью создавать и исследовать модели автоматизированных систем<br>Знать<br>– Основные информационные технологии, используемые в автоматизированных системах;<br>– Классификацию современных автоматизированных систем;<br>– Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем.<br>Уметь<br>– Демонстрировать способность и готовность к решению задач оптимизации применительно к различным предметным областям;<br>– Определять возможность применения основных положений и методов теории оптимизации для организации мер по защите информации в автоматизированных системах;<br>– Находить оптимальные стратегии.<br>Владеть<br>– Навыками использования стандартных методов теории оптимизации;<br>– Навыками использования стандартных методов и моделей математического анализа, теории оптимизации;<br>– Навыками использования стандартных методов и моделей математического анализа, теории оптимизации, а так же их применения к решению прикладных задач.<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>– Основные понятия математического анализа, дифференциальной геометрии, численные методы оптимизации<br>Уметь<br>– Самостоятельно расширять математические знания и проводить анализ прикладных задач за счет получения дополнительной информации в условиях недостающей информации;<br>– Реализовать основные алгоритмы оптимизации средствами программного обеспечения и вычислительной техники;<br>– Разрабатывать алгоритмы численного решения задач оптимизации<br>Владеть<br>– Основными методами оптимизации;<br>– Методами оптимизации средствами вычислительной техники;<br>– Навыками реализации задач оптимизации посредством | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | программного обеспечения общего назначения и методо-ориентированного программного обеспечения<br>**Дисциплина включает в себя следующие разделы:**<br>1. Предмет и содержание дисциплины<br>1.1 Введение в теорию оптимизации. Предмет и задачи исследования теории оптимизации.<br>1.2 Основные положения теории оптимизации. Основные термины и понятия.<br>2. Линейное программирование. Методы решения ЗЛП<br>2.1 Основные положения линейного программирования. Основные термины и понятия.<br>2.2 Методы решения задач линейного программирования. Графический метод. Симплексный метод.<br>3. Применение общей задачи линейного программирования для решения прикладных<br>3.1 Закрытая модель транспортной задачи. Открытая модель транспортной задачи. Постановка задачи и ее математическая модель. Программная реализация открытой и закрытой ТЗ.<br>3.2 Транспортная задача с дополнительными ограничениями. Приложения транспортной задачи для решения задач из различных предметных областей. Программная реализация задач<br>3.3 Построение математической модели для решения сетевых задач. Решение сетевых задач методами линейного программирования. Программная реализация задач<br>3.4 Решение сетевой задачи о максимальном потоке. Решение задачи о кратчайшем пути.<br>4. Решение задач комбинаторной оптимизации<br>4.1 Решение задачи о рюкзаке. Постановка задачи и ее математическая модель. Программная реализация задачи.<br>4.2 Применение задачи об укладке рюкзака к алгоритмам шифрования. Программная реализация задачи.<br>5. Моделирование систем. Решение задач одномерной оптимизации<br>5.1 Решение задач одномерной оптимизации. Методом перебора значений функции. Метод Ньютона и его модификации. Постановка задачи и ее математическая модель.<br>5.2 Решение задач одномерной оптимизации методом золотого сечения. Постановка задачи и ее математическая модель. Программная реализация задачи.<br>6. Моделирование систем. Решение задач многомерной оптимизации<br>6.1 Решение задач многомерной оптимизации методом покоординатного спуска. Постановка задачи и ее математическая модель. Программная реализация<br>6.2 Решение задач многомерной оптимизации градиентными методами. Постановка задачи и ее математическая модель. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Программная реализация<br>6.3 Использование генетических алгоритмов для решения задач многомерной оптимизации. Постановка задачи и ее математическая модель. Программная реализация задачи.<br>7. Решение прикладных задач методами оптимизации<br>7.1 Примеры решения прикладных задач методами оптимизации. Постановка задачи и ее математическая модель. Программная реализация задачи. | |
| **Б1.В.ДВ.02.02** | **Математическое моделирование распределенных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Математическое моделирование распределенных систем входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Алгебра и геометрия<br>Математический анализ<br>Математическая логика и теория алгоритмов<br>Теория вероятностей, математическая статистика<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Моделирование систем и процессов защиты информации<br>Моделирование угроз информационной безопасности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Математическое моделирование распределенных систем» обучающийся должен | *Общая трудоемкость дисциплины составляет **4** зачетных единицы **144** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | обладать следующими компетенциями:<br>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<br>Знать<br>─ теоретические основы алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов;<br>─ основные принципы и схемы автоматического управления;<br>─ основные типы систем автоматического управления, их математическое описание и основные задачи исследования систем с распределенными параметрами.<br>Уметь<br>─ применять математические методы для анализа общих свойств линейных распределенных систем;<br>─ применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами;<br>─ применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований.<br>Владеть<br>─ методами преобразования структурных схем распределенных систем управления;<br>─ методами преобразования структурных схем распределенных систем управления;<br>─ методами и навыками преобразования структурных схем распределенных систем управления.<br>ПК-2 способностью создавать и исследовать модели автоматизированных систем<br>Знать<br>─ Принципы и методы проектирования программно-аппаратного обеспечения;<br>─ Принципы и методы проектирования программно-аппаратного обеспечения;<br>─ Методы планирования и организации работ по защите информации.<br>Уметь<br>─ Разрабатывать и использовать профили защиты и задания по | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности;<br>– Готовить проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;<br>– Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы.<br>Владеть<br>– Навыками разработки технических заданий, рабочих проектов, планов и графиков проведения работ по защите информации;<br>– Навыками выполнения требований нормативно-технической документации по соблюдению установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации;<br>– Навыками проектирования программных и аппаратные средств защиты информации в соответствии с техническим заданием.<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>– Основные принципы и схемы автоматического управления;<br>– Основные требования нормативно-правовой базы в области защиты информации;<br>– Основные уязвимости защищенных компьютерных систем;<br>– Модели безопасности компьютерных систем;<br>– Методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;<br>– Математические методы для анализа общих свойств распределенных систем.<br>Уметь<br>– Проводить теоретические исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы;<br>– Применять нормативно-правовые документы в области защиты информации;<br>– Проводить теоретические и экспериментальные исследования уровня защищенности и/или оценочного уровня доверия компьютерной системы;<br>– Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем;<br>– Применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами на базе современной вычислительной техники и средств автоматизации исследований; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ Разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем<br>Владеть<br>─ Навыками выявления, исследования функциональных свойств и состояния программного обеспечения;<br>─ Навыками применения математических методов для анализа общих свойств линейных распределенных систем;<br>─ Приемами разработки математических моделей систем с распределенными параметрами;<br>─ Навыками анализа и оценки угрозы информационной безопасности объекта;<br>─ Навыками исследования алгоритма программного продукта, типов поддерживаемых аппаратных платформ;<br>─ Приемами разработки математических моделей систем с распределенными параметрами.<br>**Дисциплина включает в себя следующие разделы**<br>1. Математическое моделирование<br>1.1 Форма и принципы представления математических моделей. Моделирование как метод научного исследования. Типы моделей<br>1.2 Моделирование динамических характеристик систем с сосредоточенными параметрами<br>2. Особенности построения математических моделей<br>2.1 Подходы к построению моделей сложных систем.<br>2.2 Имитационное моделирование случайных процессов в измерительных приборах и системах.<br>2.3 Математические модели в интегральной форме.<br>2.4 Уравнения Лапласа и Пуассона. Физическая интерпретация 3 типов граничных условий. Сеточные модели и их реализация численными методами теории цепей<br>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.<br>3. Компьютерное моделирование и вычислительный эксперимент<br>3.1 Понятие псевдослучайности. Псевдослучайные объекты.<br>3.2 Базовый датчик: критерии качества, используемые методы. Генерация непрерывных случайных величин: метод отбраковки и метод обратной функции.<br>3.3 Специальные методы генерации нормально распределённых случайных величин<br>3.4 Генерация дискретных случайных величин, выборка с возвращением и выборка без возвращения.<br>3.5 Генерация случайных процессов: основные подходы. Генерация Гауссовских процессов. Решение математических моделей | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 4. Компьютерное имитационное моделирование<br>4.1 Статистическое имитационное моделирование<br>4.2 Особенности имитационного моделирования. Этапы имитационного моделирования.<br>5. Статистическое имитационное моделирование<br>5.1 Математическое моделирование стационарных физических полей в системах с распределенными параметрами.<br>5.2 Математические моделирование нестационарных полей в системах с распределенными параметрами.<br>: | |
| **Б1.В.ДВ.03** | **Дисциплины по выбору Б1.В.ДВ.03** | |
| **Б1.В.ДВ.03.01** | **Анализ безопасности информационных технологий**<br>**1 Цели освоения дисциплины (модуля)**<br>Общей целью дисциплины «Анализ безопасности информационных технологий» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Анализ безопасности информационных технологий» являются: изучить функции, методы и алгоритмы и готовые аппаратно-программные решения анализа безопасности информационных технологий; научится применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем; выполнять аудит информационной безопасности информационных систем.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Анализ безопасности информационных технологий входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Организация ЭВМ и вычислительных систем<br>Техническая защита информации<br>Виртуальные сети<br>Моделирование угроз информационной безопасности<br>Сети и системы передачи информации<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных | *Общая трудоемкость дисциплины составляет 3 зачетных единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Тестирование систем защиты информации автоматизированных систем<br>Организационное и правовое обеспечение информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Анализ безопасности информационных технологий» обучающийся должен обладать следующими компетенциями:<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- Технические требования к испытательной лаборатории;<br>- Методологией тестирования безопасности информационных технологий.<br>Уметь<br>- Развертывать уязвимые информационно-технологических ресурсы автоматизированной системы.<br>Владеть<br>-Навыками анализа безопасности информационно-технологических ресурсов автоматизированной системы.<br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы<br>Знать<br>- Принципы получения OSINT информации.<br>Уметь<br>- Выполнять тестирование автоматизированной системы с целью получения OSINT информации.<br>Владеть<br>- Навыками формирования отчета о текущем уровни безопасности автоматизированной системы<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Классификацию уязвимостей;<br>- Принципы систематизации уязвимостей.<br>Уметь<br>- Выполнять сканирование автоматизирование системы с цель выявления уязвимостей безопасности ИТ.<br>Владеть<br>- Навыками исследования уязвимостей автоматизированной системы.<br><br>**1 Цели освоения дисциплины (модуля)**<br>1. Среда для проведения анализа информационных технологий<br>1.1 Технические требования. Физическая и виртуальная испытательные лаборатории. Тестовые ИТ.<br>1.2 Параметрирование уязвимых виртуальных сервисов. Metaspoiltable2 и Metaspoiltable 3<br>2. Методология анализа безопасности информационных технологий<br>2.1 Стандарты проведения тестирования безопасности ИТ. Методика OWASP.<br>2.2 Методика PCI. NIST 800-115. Фреймворки для проведения тестирования безопасности ИТ<br>3. Получение информации о ИТ автоматизированной системы<br>3.1 Получение информации из открытых источников. Использование общих ресурсов. Анализ записей DNS<br>3.2 Получение сведений о сетевой маршрутизации. Автоматические инструменты для получения footprint и сбора информации.<br>4. Тестирование ИТ автоматизированной системы<br>4.1 Идентификация целевого сервиса. Выявление активных сетевых приложений.<br>4.2 Средства автоматического тестирования. Nmap, Netdiscover, stricker.<br>5. Исследование уязвимостей безопасностей ИТ<br>5.1 Типы уязвимостей. Классификация уязвимостей.<br>5.2 Автоматическое тестирование уязвимостей ИТ автоматизированной системы. Исследование уязвимостей.<br>6. Создание отчетов о тестировании уязвимостей безопасности ИТ<br>6.1 Тивы отчетов. Отчет о тестировании безопасности сети.<br>6.2 Автоматизированные системы генерации отчетов. Dradis. Faraday.<br>7. Зачет с оценкой | |
| **Б1.В.ДВ.03.02** | **Информационная безопасность систем организационного управления**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью изучения дисциплины «Информационная безопасность систем организационного управления» является | *Общая трудоемкость дисциплины* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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 учреждениях.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина «Информационная безопасность систем организационного управления» входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Криптографические методы защиты информации<br>Моделирование угроз информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Безопасность операционных систем<br>Информационная безопасность распределенных информационных систем<br>Методы выявления нарушений информационной безопасности<br>Аттестация АИС<br>Организационное и правовое обеспечение информационной безопасности<br>Тестирование систем защиты информации автоматизированных систем<br>Техническая защита информации<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Математическое моделирование распределенных систем<br>Основы теории оптимизации<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена | *составляет 3 зачетных единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Производственная-преддипломная практика<br>3 Компетенции обучающегося, формируемые в результате освоения<br>дисциплины (модуля) и планируемые результаты обучения<br>В результате освоения дисциплины (модуля) «Информационная безопасность систем организационного управления» обучающийся должен обладать следующими компетенциями:<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Информационная безопасность систем организационного управления» обучающийся должен обладать следующими компетенциями:<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>-основные понятия предметной области построения систем организационного управления<br>– основные критерии оценки защищенности систем организационного управления, источники угроз и нормативные документы в области защиты информации<br>-основные информационные технологии, используемые в автоматизированных системах;<br>-передовой опыт по внедрению современных организационно-технических мер, средств и способов защиты информации с целью повышения их эффективности<br>Уметь<br>-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем организационного управления<br>- моделировать потоки информации и документооборот, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности<br>-разрабатывать эксплуатационную документацию для систем организационного управления с учетом требований информационной безопасности<br>Владеть<br>-навыками применения современных информационных технологий с учетом требований информационной безопасности в системах организационного управления (ОУ)<br>-навыками подготовки инструкций по эксплуатации систем организационного управления с учетом требований | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информационной безопасности<br><br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы<br>Знать<br>-методы и средства контроля охраняемых сведений<br>- программные средства, поддерживающие управление информационной безопасностью<br>-отечественный и зарубежный опыт в области управления информационной безопасностью<br>Уметь<br>-разрабатывать политики безопасности для элементов системы ОУ<br>-расследовать инциденты ИБ<br>-разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ<br>-готовить предложения для актуализации организационных мер по защите информационных систем ОУ<br>Владеть<br>-терминологией и процессным подходом построения СУИБ.<br>-навыками определения актуальных угроз и применения мер их нейтралицации<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать<br>- основные понятия организации обеспечения информационной безопасности<br>-основные методы организации обеспечения информационной безопасности;<br>- принципы организации обеспечения информационной безопасности<br>Уметь<br>-анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития;<br>-организовывать и обеспечивать сохранение режима государственной тайны при выполнении функциональных обязанностей;<br>- организовывать и обеспечивать сохранение режима конфиденциальности при выполнении функциональных обязанностей;<br>Владеть<br>-методами формирования требований по защите объекта;<br>-методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;<br>**Дисциплина включает в себя следующие разделы:** | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1. Классификация систем ОУ<br><br>1.1. Классификация систем ОУ по функциям управления; по видам управляющих команд; по степени сосредоточения власти<br>1.2. Технологическое обеспечение, информационные процессы в автоматизированных системах организационного управления.<br>1.3. Концепции создания и развития объекта управления и системы организационного управления<br>2 Угрозы систем организационного управления<br>2.1 Анализ источников угроз и проектирование модели разграничения прав доступа для АИС ОУ<br>3.Управление правами доступа<br>3.1 Разграничение прав доступа к объектам. Ограничение доступа на интерфейсном уровне.<br>3.2 Задание доступа на уровне серверной базы данных.<br>3.3 Идентификация и профайлинг пользователей.<br>3.5 Применение аппаратных средств защиты информации в АИС организационного управления<br>4. Организация реагирования на чрезвычайные ситуации (инциденты) | |
| **Б1.В.ДВ.04** | **Дисциплины по выбору Б1.В.ДВ.04** | |
| **Б1.В.ДВ.04.01** | **Виртуальные сети**<br>**1 Цели освоения дисциплины (модуля)**<br>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».<br>Специальными целями дисциплины «Виртуальные сети» являются:<br>- изучение архитектуры и настроек виртуальных локальных сетей (VLAN);<br>- изучение структуры, принципов работы, настроек виртуальных частных сети (VPN) и технологий на их основе Site-to-site VPN, FlexVPN и SSL VPN;<br>- освоение облачных технологий виртуальных сетей.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Виртуальные сети входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Организация ЭВМ и вычислительных систем<br>Сети и системы передачи информации<br>Технология построения защищенных распределенных приложений<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Криптографические методы защиты информации<br>Знания(умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Виртуальные сети» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах;<br>- Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах.<br>Уметь<br>- Создавать защищенные вычислительные сети с применением виртуализации;<br>- Применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях.<br>Владеть<br>- Навыками разработки, документирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | требований по обеспечению безопасности.<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>-Информационно-технологические ресурсы автоматизированных систем;<br>-Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности.<br>Уметь<br>-Создавать виртуальные сети для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;<br>-Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности.<br>Владеть<br>-Навыками настройки сетевого оборудования с учетом требований информационной безопасности для эффективного применения информационно-технологических ресурсов автоматизированной системы;<br>-Навыками развертывания виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы.<br>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Знать<br>-Последовательность и содержание этапов построения виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах;<br>-Основы удаленного администрирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.<br>Уметь<br>- Создавать и администрировать виртуальные локальные сети и виртуальные частные сети, а также специализированные виртуальные сети в облачных сетевых структурах;<br>- Реализовывать политику безопасности виртуальной локальной сети и виртуальной частной сети, а также специализированной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | виртуальной сети в облачных сетевых структурах;<br>- 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.<br>Владеть<br>- 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;<br>- Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, авторизации, аутентификации и аудита), виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению информационной безопасности.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Виртуальные локальные сети (VLAN).<br>1.1 Типы VLAN, сегментация VLAN. голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet.<br>1.2 Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Поиск неисправностей при использовании VLAN.<br>1.3 Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.<br>2. Виртуальные частные сети (VPN). Сетевые технологии Site-to-site VPN, FlexVPN и SSL VPN. Настройка и исполь-зование Cisco AnyConnect VPN.<br>2.1 Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Основные компоненты VPN-технологии.<br>2.2 Протоколы работы VPN: GRE, PPTP, L2TP, PPPoE. Конфигурирование соединения<br>2.3 Протокол ISAKMP. Технология IPSec, Совместная работа IPSEC и NAT. Транзитная передача шифрованного трафика.<br>2.4 Dynamic VPN, конфигурирование функций динамического VPN-концентратора. Конфигурирование сервиса DynDNS.<br>2.5 Конфигурирование классического туннельного соединения для объединения офисных сетей. Развёртывание DMVPN на устройствах с Cisco IOS. IPSec VPN с использованием SDM.<br>2.6 Технология FlexVPN. Основные преимущества и возможности технологии FlexVPN.. Централизованное конфигурирование узлов-участников. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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<br>2.8 Настройка и использование Cisco AnyConnect VPN. Мониторинг работы AnyConnect VPN. Настройка специфических аспектов работы AnyConnect VPN.<br>3. Облачные технологии виртуальных сетей.<br>3.1 Характеристики аппаратно-программных платформ виртуализации для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS<br>3.2 Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами.<br>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).<br>3.4 Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA).<br>3.5 Создание VPN-серверов для виртуальных частных сетей в облаке.<br>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 | |
| **Б1.В.ДВ.04.02** | **Защита программного обеспечения**<br>**1 Цели освоения дисциплины (модуля)**<br>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».<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Защита программного обеспечения входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Безопасность операционных систем<br>Языки программирования | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Информатика<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Технология построения защищенных распределенных приложений<br>Технологии и методы программирования<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Защита программного обеспечения» обучающийся должен обладать следующими компетенциями:<br>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<br>Знать<br>- Современные технологии программирования.<br>- Области и особенности применения языков программирования высокого уровня;<br>- Основные виды интегрированных сред разработки программного обеспечения.<br>- Основные методы эффективного кодирования.<br>- Способы обработки исключительных ситуаций;<br>- Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.<br>Уметь<br>- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач;<br>- Работать с основными средами интегрированной разработки программного обеспечения;<br>- Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;<br>- Реализовывать разработанную структуру классов для задач предметной области.<br>Владеть | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Навыками реализации алгоритмов на языках программирования высокого уровня;<br>- Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области.<br>- Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.<br>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы<br>Знать<br>─ способы обработки исключительных ситуаций; современные технологии и методы программирования, предназначенные для создания прикладных программ;<br>─ Нормативные документы по стандартизации и сертификации программной защиты.<br>─ Цели и задачи разработки политики информационной безопасности<br>─ Методы и средства анализа достаточности мер по обеспечению ИБ ПО<br>Уметь<br>─ Разрабатывать порядок эксплуатации программного обеспечения<br>─ Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения<br>─ Проводить мониторинг и аудит защищенности ПО<br>Владеть<br>─ Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО<br>─ Методами контроля соблюдения политики учетных записей<br>─ Навыками регламентации обслуживания и осуществления модификации программного обеспечения<br>ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Знать<br>- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;<br>- основные модели данных, физическую организацию баз данных;<br>- последовательность и содержание этапов проектирования баз данных;<br>Уметь<br>- разрабатывать и администрировать базы данных в соответствии с требования информационной безопасности;<br>-настраивать защиту программного обеспечения с применением | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | дистанционного администрирования<br>Владеть<br>- методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств;<br>-в полной мере средствами администрирования БД в интегрированных средах СУБД.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение в теорию обеспечения безопасности программного обеспечения и данных<br>1.1 Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.<br>1.2 Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ<br>1.3 Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.<br>2. Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность<br>2.1 Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.<br>2.2 Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.<br>3. Методы и средства обеспечения целостности и достоверности используемого программного кода<br>3.1 Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.<br>3.2 Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу.<br>3.3 Основные подходы к защите программного обеспечения от несанкционированного копирования.<br>4. Администрирование и защита БД<br>4.1 Понятия администрирование, привилегия, доступ. Виды пользователей и группы привилегий, соответствующие виду пользователя.<br>4.2 Программные и программно-аппаратные средства защиты БД<br>4.3 Контроль доступа к данным. Управление привилегиями пользователей базы данных. Идентификация и аутентификация пользователя. Пароли.<br>4.4 Транзакционный подход к организации доступа к данным. Понятие SQL Injection. Виды уязвимостей, используемые атаками SQL Injection. Методы защиты от Injection. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 4.5 Использование аудита БД. Аудит системных событий. Системы обнаружения вторжений. | |
| **Б1.В.ДВ.05** | **Дисциплины по выбору Б1.В.ДВ.05** | |
| **Б1.В.ДВ.05.01** | **Методы мониторинга информационной безопасности АС**<br>**1 Цели освоения дисциплины (модуля)**<br>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 соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».<br>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; научится применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем; выполнять аудит информационной безопасности информационных систем.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Методы мониторинга информационной безопасности АС входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Информатика<br>Организация ЭВМ и вычислительных систем<br>Техническая защита информации<br>Моделирование систем и процессов защиты информации<br>Организационное и правовое обеспечение информационной безопасности<br>Безопасность сетей ЭВМ<br>Моделирование угроз информационной безопасности<br>Управление информационной безопасностью<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной | *Общая трудоемкость дисциплины составляет **5** зачетных единицы **180** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | работы<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Методы мониторинга информационной безопасности АС» обучающийся должен обладать следующими компетенциями:<br>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем<br>Знать<br>- способы организации автоматизированных систем;<br>- подходы к проведению сертификации средств защиты информационной безопасности;<br>Уметь<br>- составлять регламент испытаний средств защиты информации автоматизированных систем;<br>Владеть<br>- навыками применения, специализированного ПО для проведения мероприятий при сертификации средств защиты информации автоматизированных систем;<br>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации<br>Знать<br>- перечень инструментов для проведения мониторинга защищенности информации;<br>- базовый функционал инструментов для проведения мониторинга защищенности информации;<br>Уметь<br>- применять технические средства для проведения мониторинга беспроводных сетей;<br>- применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;<br>Владеть<br>- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | системы с учетом требований информационной безопасности<br>Знать<br>- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;<br>Уметь<br>- выполнять работы по оптимизации схем управления автоматизированной системой;<br>- выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;<br>Владеть<br>- навыками определения возможных векторов атаки на автоматизированную систему;<br>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем<br>Знать<br>- способы получения информации о внутренней структуре исследуемой распределенной системе;<br>-наиболее распространённые точки для несанкционированного входа в распределенную систему;<br>Уметь<br>- проводить анализ уязвимостей распределённой системы;<br>- получать несанкционированный доступ к ресурсам распределенной системы;<br>Владеть<br>- навыками противодействия внешним атакам на распределенную информационную сеть;<br>**Дисциплина включает в себя следующие разделы:**<br>1. Введение в мониторинг АС<br>1.1 Архитектура и функции систем мониторинга информационной безопасности.<br>1.2 Модульный принцип построения системы информационной безопасности.<br>2. Мониторинг ИБ АС<br>2.1 Идентификация пользователей, трафика, приложений, протоколов и схем использования ресурсов.<br>2.2 Ограничение доступа и использования ресурсов на уровне пользователя, протокола, сервиса и приложения. Изоляция пользователей, сервисов и приложений<br>3. Средства мониторинга ИБ АС<br>3.1 Применение специализированных дистрибутивов Linux для создания АРМ системы мониторинга ИБ АС<br>3.2 Установка и настройка дистрибутива Kali Linux 2<br>4. Аудит проводных сетей<br>4.1 Способы организации зеркалирования трафика. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 4.2 Способы обнаружения угроз по сетевой активности<br>5. Аудит беспроводных сетей<br>5.1 Получение доступа к беспроводной сети<br>5.2 Способы противодействия атакам на беспроводную сеть<br>6. Аудит Web-ресурсов<br>6.1 Аудит средств авторизации<br>6.2 Защита от SQL инъекций | |
| **Б1.В.ДВ.05.02** | **Защита электронного документооборота**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Защита электронного документооборота входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Криптографические методы защиты информации<br>Моделирование угроз информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Безопасность операционных систем<br>Информационная безопасность распределенных информационных систем<br>Методы выявления нарушений информационной безопасности<br>Организационное и правовое обеспечение информационной безопасности<br>Тестирование систем защиты информации автоматизированных систем<br>Техническая защита информации<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Математическое моделирование распределенных систем<br>Основы теории оптимизации | *Общая трудоемкость дисциплины составляет **5** зачетных единицы **180** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Программно-аппаратные средства обеспечения информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Научно-исследовательская работа<br>Подготовка к защите и защита выпускной квалификационной работы<br>Подготовка к сдаче и сдача государственного экзамена<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения**<br>**дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Защита электронного документооборота» обучающийся должен обладать следующими компетенциями:<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- основные понятия предметной области систем электронного документооборота<br>-основные информационные технологии, используемые в автоматизированных системах;<br>− принципы построения и функционирования, примеры реализаций систем электронного документооборота;<br>нормативные правовые акты в области защиты информации<br>Уметь<br>-применять современные информационные технологии для поиска, прохождения, обработки, учета и рассылки информации внутри систем электронного документооборота<br>- моделировать потоки информации и документов, в корпоративных информационных системах и осуществлять их оценивание с точки зрения информационной безопасности<br>-готовить научно-технические отчеты, обзоры, публикации по теме предметной области<br>Владеть<br>-навыками применения современных информационных технологий для поиска, прохождения, обработки, учета и рассылки документов внутри систем электронного документооборота<br>-навыками моделирования потоков информации в корпоративных информационных системах и выявления актуальных угроз ИБ<br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Знать<br>-нормативные акты, используемые при разработке политики информационной безопасностью организации;<br>– основные критерии оценки защищенности систем электронного документооборота, источники угроз<br>методические рекомендации отраслевых регуляторов по обеспечению информационной безопасности<br>Уметь<br>- проводить сбор и анализ данных о состоянии защиты информации в организации; оценку рисков ИБ;<br>применять государственные стандарты и методические рекомендации для построения СЗИ организации<br>разрабатывать политики информационной безопасности для систем электронного документооборота<br>Владеть<br>- навыками разработки политик информационной безопасности для систем электронного документооборота<br>-методами моделирования потоков информации, документооборота АИС<br>- навыками анализа данных о состоянии систем защиты информации в организации; оценки информационных оценки рисков;<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать<br>– принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечению информационной безопасности<br><br>Уметь<br>-выявлять особенности и формировать требования к системе организации коллективной работы с информационными ресурсами СЭД<br>-формировать комплекс мер по защите информации с учетом соответствия нормативным документам, технической реализуемости и экономической целесообразности;<br><br>Владеть<br>-навыками администрирования систем электронного документооборота<br>-навыками настройки систем предотвращения утечек информации<br><br>**Дисциплина включает в себя следующие разделы**: | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 1. Функции, задачи и особенности электронного документооборота<br><br>1.1 Основные понятия и принципы электронного документооборота. Теоретические и организационные основы создания систем электронного документооборота организации.<br>1.2 Методологические основы разработки информационной системы электронного документооборота. Классификация систем электронного документооборота. Государственные услуги, банковское обслуживание, электронные закупки.<br>1.3 Применение нормативно-правовых актов по защите информации в СЭДО.<br>ГОСТ Р 53898-2010<br>1. Угрозы безопасности для систем электронного документооборота<br><br>2.2 Угрозы целостности и доступности СЭДО. Угроза доступа сервера ОС. Угроза сервера СЭД. Контроль целостности электронного документа.<br>2.1 Угроза конфиденциальности. Угроза доступа рабочих мест. Угроза доступа сервера ОС. Угроза сервера СЭД. Угроза перехвата каналов связи<br>3. Проблемы применения ЭЦП в системах электронного документооборота<br>3.1 Проблемы подлинности документов в системе ЭДО. Применение Электронно-цифровой подписи в соответствии с уровнем юридической значимости документа.<br>3.2 Регламент использования электронных средств обмена документами в зависимости от уровня взаимодействия(внутри организации, межорганизационный, межведомственный)<br>3.3 Проблемы «отчуждения» ключей электронной подписи и возможные способы их решения<br>4. Проблемы аутентификации пользователей систем электронного документооборота<br>4.1 Разграничение прав доступа к объектам. Ограничение доступа на интерфейсном уровне.<br><br>5. Использование DLP – систем для предотвращения утечек СЭД<br>5.1 Обзор и сравнение российских и зарубежных dlp-систем.<br>5.2 Идентификация и профайлинг пользователей пользователей. Создание правил безопасности.<br>5.3 Фильтрация трафика при перехвате. Организация защищенной системы электронной почты. Цифровые отпечатки<br>5.4 Оценка эффективности защиты СЭД. Оценка по экономической эффективности. Методы оценки по интегральному эффекту («линейная свертка» частных показателей, методы теории нечетких множеств). | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 6. Аппаратная защита технологии электронного обмена информацией<br>6.1 Применение аппаратных средств защиты информации в системах электронного документооборота.<br>7. Проектирование и внедрение защищенного электронного документооборота<br>7.1 Проектирование организационных, программных, аппаратных и иных средств СЗИ. Особенности эксплуатации защищенных систем электронного документооборота.<br>7.2 Анализ эффективности и разработка мер по совершенствованию СЗИ СЭД. | |
| **Б2** | **Практики** | |
| **Б2.Б** | **Базовая часть** | |
| **Б2.Б.01(У)** | **Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности**<br>**1 Цели практики/НИР**<br>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.<br>**2 Задачи практики/НИР**<br>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.<br>**3 Место практики/НИР в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Для прохождения практики необходимы знания (умения, владения), результате изучения дисциплин/ практик:<br>Информатика<br>Введение в специальность<br>Теория информации<br>Организация ЭВМ и вычислительных систем<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Языки программирования<br>Знания (умения, владения), полученные в процессе прохождения пр необходимы для изучения дисциплин/практик:<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Безопасность операционных систем<br>Программно-аппаратные средства обеспечения информационной бе<br>Разработка и эксплуатация защищенных автоматизированных систе<br>Техническая защита информации<br>Технология построения защищенных распределенных приложений<br>Информационная безопасность распределенных информационных с<br>Криптографические методы защиты информации<br><br>**4 Место проведения практики/НИР**<br>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»<br>Способ проведения практики/НИР: стационарная<br>Практика/НИР осуществляется дискретно<br>**5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения**<br>В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями:<br>ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач<br>Знать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Основные физические явления и процессы, имеющие отношение к профессиональной деятельности<br>- Физические основы функционирования систем обработки и передачи информации.<br>Уметь<br>- Определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач<br>- Анализировать физические явления и процессы формализации и решения профессиональных задач<br>Владеть<br>- основными методами математической формализации<br>- методами анализа физических явлений и процессов при решении профессиональных задач<br>- средствами анализа физических явлений и процессов для формализации и решения профессиональных задач<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>- Синтаксис языков программирования высокого уровня (объектно-ориентированное программирование);<br>- Современные технологии и методы программирования;<br>- Показатели качества программного обеспечения;<br>- Методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;<br>- Принципы организации документирования разработки, процесса сопровождения программного обеспечения.<br>Уметь<br>- Работать с интегрированной средой разработки программного обеспечения;<br>- Реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;<br>- Проводить комплексное тестирование и отладку программных систем;<br>- Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;<br>- Проводить выбор эффективных способов решения профессиональных задач;<br>- Планировать разработку сложного программного обеспечения;<br>- Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;<br>автоматизированных систем;<br>Владеть | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Навыками программирования различными стилями.<br>- Навыками разработки программной документации.<br>- Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.<br>- Навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования.<br>ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах<br>Знать<br>─ Основные понятия информатики;<br>─ Основные способы хранения, обработки и передачи информации;<br>─ Основы технологии поиска в современных информационно-поисковых системах;<br>─ Значение информации в развитии современного общества.<br>Уметь<br>─ Пользоваться сетевыми средствами для обмена данными, с использованием глобальной информационной сети Интернет;<br>─ Применять функции офисных приложений для организации поиска информации по заданным критериям;<br>─ Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач.<br>Владеть<br>─ Навыками использования современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах при решении профессиональных задач;<br>─ Навыками построения запросов для организации поиска информации в компьютерных системах, сетях, библиотечных фондах.<br>ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий<br>Знать<br>─ принципы построения и функционирования, примеры реализаций современных операционных систем;<br>─ принципы работы элементов и функциональных узлов электронной аппаратуры;<br>─ типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br>- Принципы адресации в вычислительных сетях;<br>- Принципы организации межсетевого взаимодействия и межсетевой передачи информации | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Уметь<br>─ применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска);<br>─ работать с современной элементной базой электронной аппаратуры<br>- Выбирать требуемое сетевое и телекоммуникационное оборудование, необходимое для организации вычислительной сети с требуемыми характеристиками<br>Владеть<br>─ навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;<br>─ Профессиональным языком и терминологией предметной области<br>─ Современным сетевым оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей<br>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<br>Знать<br>- Основы построения систем обработки и передачи информации, их современное состояние развития.<br>-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<br>- Особенности обработки информации с использованием компьютерных систем<br>Уметь<br>- Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>- Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>Владеть<br>- Навыками сбора современной научно-технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>- Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам<br>ОК-5 способностью понимать социальную значимость своей | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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<br>Знать<br>- политику государства в области обеспечения информационной безопасности<br>- национальные, межгосударственные и международные стандарты в области защиты информации<br>- современное состояние рынка труда в области обеспечения информационной безопасности<br>- профессиональный стандарт «Специалист по защите информации в автоматизированных системах»<br>- трудовое законодательство РФ<br>Уметь<br>- анализировать информацию по вопросам национальной и информационной безопасности государства;<br>- соблюдать нормы профессиональной этики<br>Владеть<br>- профессиональной терминологией в области информационной безопасности;<br>- практическими навыками соблюдения норм профессиональной этики<br>**Практика включает в себя следующие разделы**:<br>1. Подготовительный (ознакомительный).<br>2. Экспериментально- исследовательский<br>3. Обработка и анализ полученной информации.<br>4. Отчетный | |
| **Б2.Б.02(Н)** | **Научно-исследовательская работа**<br>**1 Цели практики/НИР**<br>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.<br>**2 Задачи практики/НИР**<br>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 | *Общая трудоемкость дисциплины составляет **15** зачетных единицы **540** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информации<br>**3 Место практики/НИР в структуре образовательной программы**<br>Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Анализ рисков информационной безопасности<br>Методы мониторинга информационной безопасности АС<br>Методы проектирования систем защиты распределенных информационных систем<br>Моделирование систем и процессов защиты информации<br>Управление информационной безопасностью<br>Знания (умения, владения), полученные в процессе прохождения практики/НИР будут необходимы для изучения дисциплин/практик:<br>Подготовка к защите и защита выпускной квалификационной работы<br>Производственная-преддипломная практика<br>Подготовка к сдаче и сдача государственного экзамена<br><br>**4 Место проведения практики/НИР**<br>Способ проведения практики/НИР: выездная стационарная<br>Практика/НИР осуществляется дискретно<br>**5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения**<br>В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями:<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>- нормативные правовые акты в области защиты информации;<br>- национальные, межгосударственные и международные стандарты в области защиты информации;<br>- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.<br>- порядок разработки модели угроз<br>− цели и задачи моделирования систем и процессов защиты информации;<br>- способы обеспечения информационной безопасности информационных систем; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - основные принципы построения моделей систем защиты информации<br>- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем<br>Уметь<br>- обосновать выбор подходящего метода и привести алгоритм решения задачи;<br>- формировать множество альтернативных решений, ставить цель и выбирать оценочный критерий оптимальности способа решения<br>- применять новые технологии проектирования и анализа систем<br>- проводить мониторинг угроз безопасности информационных систем<br>Владеть<br>- навыками решения моделирования процессов защиты информации<br>- навыками проектирования информационных структур<br>- навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения<br>- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;<br>− навыками анализа основных узлов и устройств современных автоматизированных систем<br>ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами<br>Знать<br>Основные подходы координирования специалистов по защите информации на предприятии, в учреждении, организации.<br>Этапы создания междисциплинарных и инновационных проектов.<br>Уметь<br>Участвовать в деятельность специалистов по ЗИ на предприятии, в учреждении, организации.<br>Координировать деятельность подразделений по ЗИ на предприятии, в учреждении, организации.<br>Принимать участие в междисциплинарных и инновационных проектах<br>Владеть<br>Методиками руководства подразделений по ЗИ на предприятии, в учреждении, организации.<br>Навыками организации и реализации междисциплинарных и инновационных проектов<br>ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке<br>Знать<br>Основы построения систем обработки и передачи информации, их современное состояние развития.<br>Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.<br>Особенности обработки информации с использованием компьютерных систем<br>Уметь<br>Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Принимать участие в исследованиях и анализе современной научно- технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Владеть<br>Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Навыками участия в проведении исследовательских работ по рассматриваемым в рамках дисциплины проблемам и задачам.<br>Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач.<br>ПК-2 способностью создавать и исследовать модели автоматизированных систем<br>Знать<br>-основные принципы моделирования и виды моделей, требования, предъявляемые к моделям<br>-методы оценки качества моделей, методы и средства моделирования и оптимизации бизнес-процессов<br>-основные угрозы безопасности информации и модели нарушителя в автоматизированных системах<br>-способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах<br>Уметь<br>-строить и изучать компьютерные модели конкретных явлений и процессов для решения расчетных и исследовательских задач<br>-применять различные методы моделирования, исследования и верификации моделей<br>-разрабатывать постановку задачи моделирования и выбирать методы и средства моделирования систем защиты информации<br>− анализировать и оценивать угрозы информационной безопасности объекта; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | − разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем<br>Владеть<br>-навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач<br>-навыками формализации задач и постановки задач моделирования<br>-навыками выбора и обоснования критериев эффективности функционирования моделей<br>-навыками разработки, документирования информационных систем с учетом требований по обеспечению информационной безопасности;<br>-навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите<br>-методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>источники и классификацию угроз информационной безопасности;<br>основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;<br>Уметь<br>анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;<br>классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;<br>Владеть<br>навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;<br>методами формирования требований по защите информации;<br>навыками анализа основных узлов и устройств современных автоматизированных систем;<br>навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем<br>ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ<br>Знать<br>нормативные правовые акты и нормативные методические | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | документы в области обеспечения информационной безопасности, структуру научно-технических отчетов<br>Уметь<br>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;<br>применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>Владеть<br>способностью разрабатывать научно-техническую документацию<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>Знать<br>Средства анализа информационной безопасности;<br>Классификацию систем защиты информации;<br>Средства организации аттестации ВП по требованиям безопасности информации.<br>Уметь<br>Принимать участие в исследованиях аттестации системы защиты информации;<br>Принимать участие в исследованиях и анализе аттестации системы защиты информации;<br>Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.<br>Владеть<br>Навыками использования средств анализа информационной безопасности;<br>Навыками участия в проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности;<br>Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;<br>Уметь<br>выполнять работы по оптимизации схем управления автоматизированной системой; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы<br>выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень информационной безопасности;<br>Владеть<br>навыками определения возможных векторов атаки на автоматизированную систему; и осуществлять выбор средств защиты информации<br>**Научно-исследовательская работа включает следующие разделы:**<br>1. Планирование научно-исследовательской работы, включающее ознакомление с тематикой исследовательских работ в области информационной безопасности, выбор темы исследования подготовка литературного обзора<br>2. Проведение научно-исследовательской работы<br>3. Составление отчета о научно-исследовательской работе<br>4. Защита выполненной работы | |
| **Б2.Б.03(П)** | **Производственная практика по получению профессиональных умений и опыта профессиональной деятельности**<br>**1 Цели практики**<br>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.<br>**2 Задачи практики**<br>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 | *Общая трудоемкость дисциплины составляет **6** зачетных единицы **216** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | первоначального практического опыта.<br>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.<br>**3 Место практики в структуре образовательной программы**<br>Для прохождения практики необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Языки программирования<br>Сети и системы передачи информации<br>Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности<br>Основы информационной безопасности<br>Технология построения защищенных распределенных приложений<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Техническая защита информации<br>Организационное и правовое обеспечение информационной безопасности<br>Информационная безопасность распределенных информационных систем<br>Безопасность операционных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Методы мониторинга информационной безопасности АС<br>Криптографические методы защиты информации<br>Знания (умения, владения), полученные в процессе прохождения практики будут необходимы для изучения дисциплин/практик:<br>Анализ рисков информационной безопасности<br>Виртуальные сети<br>**4 Место проведения практики**<br>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 | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>Способ проведения практики: выездная и/или стационарная<br>Практика осуществляется дискретно<br>**5 Компетенции обучающегося, формируемые в результате прохождения практики и планируемые результаты обучения**<br>В результате прохождения практики обучающийся должен обладать следующими компетенциями:<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>- нормативные правовые акты в области защиты информации;<br>- национальные, межгосударственные и международные стандарты в области защиты информации;<br>- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.<br>- порядок разработки модели угроз<br>- виды нарушителей информационной безопасности<br>Уметь<br>- оценивать информационные риски в автоматизированных системах;<br>- классифицировать и оценивать угрозы безопасности информации;<br>- определять подлежащие защите информационные ресурсы автоматизированных систем;<br>- анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации<br>- оценивать потенциал нарушителя информационной безопасности<br>- применять базовую модель угроз ПДн<br>Владеть<br>- методами выявления угроз безопасности информации в автоматизированных системах;<br>- методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.<br>- навыками применения базовой модели угроз ПДн<br>ПСК-7.2 способностью проводить анализ рисков информационной | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах<br>Знать<br>- Порядок разработки политик безопасности;<br>- методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;<br>Уметь<br>- оценивать информационные риски в автоматизированных системах;<br>- выполнять анализ рисков информационной безопасности в распределенных информационных системах;<br>- анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.<br>- определить перечень необходимых политик безопасности<br>Владеть<br>- методиками проведения анализа рисков информационной безопасности распределенных информационных систем;<br>- методами оценки информационных рисков;<br>- навыками разработки политики информационной безопасности автоматизированных систем.<br>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем<br>Знать<br>─ Источники и классификацию угроз информационной безопасности;<br>─ Основные принципы построения систем защиты информации;<br>─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.<br>─ Методы и порядок проведения аудита защищенности информационно- технологических ресурсов<br>Уметь<br>─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем;<br>─ Проводить аудит защищенности информационно-технологических ресурсов<br>Владеть<br>─ Методами выявления угроз информационной безопасности автоматизированных систем;<br>─ Методами аудита уровня защищенности АИС. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ПСК-7.4 способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Знать<br>- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;<br>- основные модели данных, физическую организацию баз данных;<br>- последовательность и содержание этапов проектирования баз данных;<br>- основные средства и методы удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах<br>Уметь<br>- разрабатывать и администрировать базы данных в соответствии с требования информационной безопасности;<br>-настраивать защиту программного обеспечения с применением дистанционного администрирования<br>-настраивать удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах<br>Владеть<br>- методами настройки безопасной работы с БД с помощью современных образцов программных, технических средств;<br>-в полной мере средствами администрирования БД в интегрированных средах СУБД.<br>-средствами удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах<br>-навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать<br>-основные методы организации обеспечения информационной безопасности;<br>- принципы организации обеспечения информационной безопасности<br>- организационные меры защиты информации<br>Уметь<br>-анализировать эффективность систем защиты информации и разрабатывать направления ее развития;<br>-организовывать и обеспечивать сохранение режима государственной тайны;<br>- организовывать и обеспечивать сохранение режима конфиденциальности; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | -формировать требования к защите информации, содержащейся в информационной системе<br>-определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации<br>Владеть<br>-методами формирования требований по защите объекта;<br>-навыками разработки организационно-распорядительных документов<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>-Общие принципы построения современных языков программирования высокого уровня.<br>-Язык программирования высокого уровня (объектно-ориентированное программирование).<br>Уметь<br>-Работать с интегрированной средой разработки программного обеспечения.<br>-Использовать шаблоны классов и средства макрообработки.<br>-Использовать динамически подключаемые библиотеки.<br>-Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.<br>Владеть<br>-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования.<br>-Навыками работы с интегрированной средой разработки программного обеспечения.<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>-основы организационного и правового обеспечения информационной безопасности,<br>-основные нормативные правовые акты в области обеспечения информационной безопасности<br>- нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>Владеть<br>-навыками работы с нормативными правовыми актами<br>ОПК-8 способностью к освоению новых образцов программных, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | технических средств и информационных технологий<br>Знать<br>-Классификацию современных программных и программноаппаратных СЗИ.<br>-Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ.<br>-Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.<br>Уметь<br>-Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий.<br>-Основные принципы работы всех подсистем системы ИБ АС.<br>Владеть<br>- Навыками работы с подсистемами системы информационной безопасности автоматизированной системы.<br>- Навыками администрирования системы ИБ АС.<br>ПК-3 способностью проводить анализ защищенности автоматизированных систем<br>Знать<br>- Критерии оценки эффективности и надежности средств защиты распределенных информационных систем<br>- Принципы построения и функционирования распределенных информационных систем в защищённом исполнении<br>-Мероприятия для обеспечения защиты информации<br>Уметь<br>-Анализировать техническую и сопроводительную документацию по обеспечению ИБ.<br>-Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.<br>-Проводить контроль за событиями безопасности и действиями пользователей в информационной системе<br>-Проводить анализ и оценку функционирования системы защиты информации информационной системы<br>Владеть<br>-Навыками выбора средств защиты информации<br>-Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе<br>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Знать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | -Базовую модель угроз ПДн<br>-Нормативно-методические документы в области моделирования угроз<br>-Способы реализации угроз безопасности информации<br>-Типы нарушителя информационной безопасности в автоматизированных системах<br>-Методику разработки модели угроз<br>Уметь<br>-Разрабатывать частную модель угроз автоматизированной системы<br>-Определять актуальные угрозы для автоматизированной системы;<br>-Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.<br>Владеть<br>- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите;<br>- Навыками разработки частных моделей угроз<br>ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы<br>Знать<br>- методологию анализа рисков информационной безопасности;<br>- методики определения информационно-технологических ресурсов, подлежащих защите;<br>Уметь<br>- выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.<br>-оценить риски информационной безопасности автоматизированной системы<br>Владеть<br>- навыками анализа рисков информационной безопасности автоматизированных систем<br>-методиками анализа рисков<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>─ источники и классификацию угроз информационной безопасности;<br>─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>─ основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Уметь<br>─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;<br>─ классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;<br>─определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения<br>поддерживать конфигурацию информационной системы и ее системы защиты информации<br>Владеть<br>─ навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации<br>─ методами формирования требований по защите информации;<br>─ навыками анализа основных узлов и устройств современных автоматизированных систем;<br>─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем<br>─ навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы<br>ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ<br>Знать<br>-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов<br>Уметь<br>-принимать участие в разработке проектов нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;<br>- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>Владеть<br>-навыками разработки научно-техническую документации, научно-технических отчетов по результатом выполненных работ<br>ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем<br>Знать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ современную нормативно-правовую базу создания защищенных распределенных информационных систем;<br>─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей<br>Уметь<br>─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;<br>─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем<br>Владеть<br>─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ навыками разработки комплексной инфраструктуры защищенной информационной системы;<br>─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>- Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем<br>- Основные принципы построения защищенных распределенных компьютерных систем<br>- Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах.<br>- Современные принципы построения архитектуры ИС.<br>Уметь<br>- Осуществлять анализ несложных процессов проектирования;<br>- Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования средств защиты информации компьютерной системы<br>- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов<br>Владеть<br>- Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации<br>- Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Определять уровни защищенности и доверия программно-аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем<br>- Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации<br>- Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем;<br>- Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах<br>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<br>Знать<br>- Современные технологии программирования.<br>- Основные виды интегрированных сред разработки программного обеспечения.<br>- Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.<br>- Принципы работы элементов и функциональных узлов электронной аппаратуры;<br>-Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br>- Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;<br>Уметь<br>- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач;<br>- Работать с основными средами интегрированной разработки программного обеспечения;<br>- Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;<br>- Реализовывать разработанную структуру классов для задач предметной области.<br>-Работать с современной элементной базой электронной аппаратуры;<br>-Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации | |

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

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | информации.<br>- Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.<br>- Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.<br>Уметь<br>- Участвовать в настройке технических средств обеспечения информационной безопасности.<br>- Самостоятельно настраивать технические средства обеспечения информационной безопасности.<br>- Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации.<br>- Применять технические средства обеспечения информационной безопасности.<br>- Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ.<br>- Применять программные и программно-аппаратные средства обеспечения ИБ.<br>Владеть<br>- Техникой настройки технических средств обеспечения информационной безопасности<br>- Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем.<br>- Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.<br>- Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.<br>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем<br>Знать<br>-уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий;<br>- положение о системе сертификации средств защиты информации;<br>-продукцию, которую необходимо сертифицировать;<br>-состав участников системы сертификации и их основные функции;<br>-этапы сертификации;<br>- требования к проведению испытаний СЗИ;<br>-порядок проведения сертификационных испытаний | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Уметь<br>─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия;<br>─ проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия<br>─ проводить анализ сертификата соответствия.<br>Владеть<br>─ нормативно-правовой базой в области сертификации средств защиты информации<br>─навыками проведения испытаний средств защиты информации,<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>Знать<br>─ Средства анализа информационной безопасности;<br>─ Классификацию систем защиты информации;<br>─ Средства организации аттестации по требованиям безопасности информации<br>Уметь<br>─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов;<br>─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.<br>Владеть<br>─ Навыками использования средств анализа информационной безопасности;<br>─ Навыками проведения аттестации в соответствии с существующими нормативами.<br>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации<br>Знать<br>- перечень инструментов для проведения мониторинга защищенности информации;<br>- базовый функционал инструментов для проведения мониторинга защищенности информации;<br>Уметь<br>- применять технические средства для проведения мониторинга беспроводных сетей;<br>- применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;<br>Владеть | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;<br>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности<br>Знать<br>-организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации<br>-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;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>-анализировать и обобщения информации на стадии принятия и реализации управленческого решения,<br>-пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров<br>Владеть<br>-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований,<br>-методами организации и управления деятельностью служб защиты информации на предприятии<br>-навыками организации и обеспечения режима секретности<br>-навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов<br>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- нормативные методические документы ФСТЭК России в области ИБ;<br>- основные принципы создания системы управления информационной безопасностью.<br>- методы реализации системы управления безопасностью<br>Уметь<br>- проводить оценку информационных рисков,<br>- обосновывать решения по обеспечению ИБ объектов в | |

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности;<br>─ 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;<br>Уметь<br>─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;<br>─ разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности;<br>─ разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем<br>Владеть<br>─ навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;<br>─ нормативными требованиями по защите информации;<br>─ навыками организации и обеспечения режима секретности<br>─ навыками разработки организационно-распорядительных документов<br>ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации<br>Знать<br>- основные угрозы безопасности информации и модели нарушителя ОИ;<br>- принципы формирования политики информационной безопасности организации.<br>- способы контроля эффективности реализации политики информационной безопаности<br>Уметь<br>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- разрабатывать частные политики ИБ АС;<br>- контролировать эффективность принятых мер по реализации частных политик ИБ АС. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>- навыками разработки политик безопасности различных уровней.<br>- навыками и методами контроля эффективности сформированной политики информационной безопасности<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа<br>Знать<br>- Методы формирования требований по защите информации ограниченного доступа<br>- Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа<br>- Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.<br>- Организационные меры по защите информации ограниченного доступа<br>Уметь<br>- Использовать методы формирования требований по защите информации ограниченного доступа<br>- Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа<br>Владеть<br>- Методами формирования требований по защите информации ограниченного доступа<br>- Навыками анализа методов формирования требований по защите информации ограниченного доступа<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;<br>Уметь<br>- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы<br>- выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации<br>Владеть<br>- навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации;<br>ПК-25 способностью обеспечить эффективное применение средств | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций<br>Знать<br>- Принципы администрирования баз данных. Средства обеспечения безопасности данных.<br>- Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных<br>Уметь<br>- Анализировать работоспособность базы данных.<br>- Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД.<br>- Самостоятельно применять средства обеспечения безопасности данных.<br>- Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций.<br>- Организовывать безопасность систем баз данных<br>- Выявлять инциденты и реагировать на них<br>- Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации<br>Владеть<br>- Основными средствами обеспечения безопасности данных.<br>- Навыками работы с нормативными документами по администрированию баз данных.<br>- Средствами обеспечения безопасности данных.<br>- Навыками разработки и администрирования базы данных.<br>- Навыками организации безопасности систем баз данных.<br>- Средствами обеспечения безопасности данных и АИС.<br>- Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации<br>- Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий<br>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы<br>Знать<br>─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем;<br>─ Принципы администрирования системы информационной безопасности автоматизированной системы.<br>Уметь<br>─ Настраивать систему информационной безопасности автоматизированной системы;<br>─ Настраивать подсистемы системы информационной | |

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

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - основные принципы создания системы управления информационной безопасностью<br>Уметь<br>-разрабатывать политики безопасности для элементов системы ОУ<br>-расследовать инциденты ИБ<br>-разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ<br>-готовить предложения для актуализации организационных мер по защите информационных систем<br>- разрабатывать профили защиты<br>Владеть<br>- терминологией и процессным подходом построения СУИБ.<br>-навыками определения актуальных угроз и применения мер их нейтрализации<br>- навыками составления технических политик безопасности<br>**Практика включает в себя следующие разделы**:<br>1. Подготовительный (ознакомительный)<br>2. Экспериментально- исследовательский<br>3. Обработка и анализ полученной информации.<br>4. Отчетный | |
| **Б2.Б.04(П)** | **Производственная преддипломная практика**<br>**1 Цели практики**<br>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.<br>**2 Задачи практики**<br>Задачами производственной преддипломной практики являются закрепление, расширение, углубление и систематизацию знаний, полученных при изучении дисциплин базовой и вариативной части, на основе изучения деятельности конкретной организации, приобретение практического опыта, а также обобщение и систематизация разделов выпускной квалификационной работы. | *Общая трудоемкость дисциплины составляет **6** зачетных единицы **216** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>**3 Место практики в структуре образовательной программы**<br>Для прохождения практики необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Организация ЭВМ и вычислительных систем<br>Информатика<br>Сети и системы передачи информации<br>Основы информационной безопасности<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Техническая защита информации<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Информационная безопасность распределенных информационных систем<br>Безопасность операционных систем<br>Организационное и правовое обеспечение информационной безопасности<br>Тестирование систем защиты информации автоматизированных систем<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Разработка эксплуатационной документации на системы защиты информации автоматизированных систем<br>Основы управленческой деятельности<br>Криптографические методы защиты информации<br>Моделирование угроз информационной безопасности<br>Управление информационной безопасностью<br>Методы мониторинга информационной безопасности АС<br>Информационная безопасность систем организационного управления<br>Защита электронного документооборота<br>Защита программного обеспечения<br>**4 Место проведения практики**<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности проводится на базе кафедры «Информатики и информационной безопасности», в лабораториях технических | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 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.<br>Способ проведения практики: выездная и/или стационарная<br>Практика осуществляется дискретно<br>**5 Компетенции обучающегося, формируемые в результате прохождения практики и планируемые результаты обучения**<br>В результате прохождения практики обучающийся должен обладать следующими компетенциями:<br>ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах<br>Знать<br>- нормативные правовые акты в области защиты информации;<br>- национальные, межгосударственные и международные стандарты в области защиты информации;<br>- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.<br>- порядок разработки модели угроз<br>- виды нарушителей информационной безопасности<br>Уметь<br>- оценивать информационные риски в автоматизированных системах;<br>- классифицировать и оценивать угрозы безопасности информации;<br>- определять подлежащие защите информационные ресурсы автоматизированных систем;<br>- анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации<br>- оценивать потенциал нарушителя информационной безопасности<br>- применять базовую модель угроз ПДн<br>Владеть<br>- методами выявления угроз безопасности информации в автоматизированных системах;<br>- методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.<br>- навыками применения базовой модели угроз ПДн | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах<br>Знать<br>- Порядок разработки политик безопасности;<br>- методы и процедуры выявления угроз информационной безопасности в защищённых распределённых системах;<br>Уметь<br>- оценивать информационные риски в автоматизированных системах;<br>- выполнять анализ рисков информационной безопасности в распределенных информационных системах;<br>- анализировать и оценивать угрозы информационной безопасности объекта, выполнять анализ рисков информационной безопасности в распределенных информационных системах.<br>- определить перечень необходимых политик безопасности<br>Владеть<br>- методиками проведения анализа рисков информационной безопасности распределенных информационных систем;<br>- методами оценки информационных рисков;<br>- навыками разработки политики информационной безопасности автоматизированных систем.<br>ПСК-7.3 способностью проводить аудит защищенности информационно- технологических ресурсов распределенных информационных систем<br>Знать<br>─ Источники и классификацию угроз информационной безопасности;<br>─ Основные принципы построения систем защиты информации;<br>─ Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.<br>─ Методы и порядок проведения аудита защищенности информационно- технологических ресурсов<br>Уметь<br>─ Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;<br>─ Участвовать в проведении мониторинга угроз безопасности автоматизированных систем;<br>─ Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем;<br>─ Проводить аудит защищенности информационно-технологических ресурсов<br>Владеть<br>─ Методами выявления угроз информационной безопасности автоматизированных систем; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ Методами аудита уровня защищенности АИС.<br>ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении<br>Знать<br>-основные методы организации обеспечения информационной безопасности;<br>- принципы организации обеспечения информационной безопасности<br>- организационные меры защиты информации<br>Уметь<br>-анализировать эффективность систем защиты информации и разрабатывать направления ее развития;<br>-организовывать и обеспечивать сохранение режима государственной тайны;<br>- организовывать и обеспечивать сохранение режима конфиденциальности;<br>-формировать требования к защите информации, содержащейся в информационной системе<br>-определить цели и задач защиты информации в информационной системе, основные этапы создания системы защиты информации<br>Владеть<br>-методами формирования требований по защите объекта;<br>-навыками разработки организационно-распорядительных документов<br>ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия<br>Знать<br>-принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов<br>-принципы и алгоритм принятия решений в нестандартных ситуациях, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия<br>-о социальных, этнических, конфессиональных и культурных особенностях представителей тех или иных социальных общностей<br>Уметь<br>-работать в коллективе, эффективно выполнять задачи профессиональной деятельности<br>-находить организационно - управленческие решения в нестандартных ситуациях<br>-работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>-приемами взаимодействия с сотрудниками, выполняющими различные профессиональные задачи и обязанности<br>-навыками находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность<br>-способами и приемами предотвращения возможных конфликтных ситуаций в процессе профессиональной деятельности<br>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности<br>Знать<br>-Общие принципы построения современных языков программирования высокого уровня.<br>-Язык программирования высокого уровня (объектно-ориентированное программирование).<br>Уметь<br>-Работать с интегрированной средой разработки программного обеспечения.<br>-Использовать шаблоны классов и средства макрообработки.<br>-Использовать динамически подключаемые библиотеки.<br>-Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.<br>Владеть<br>-Навыками реализации основных структур данных и базовых алгоритмов средствами языков программирования.<br>-Навыками работы с интегрированной средой разработки программного обеспечения.<br>ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности<br>Знать<br>-основы организационного и правового обеспечения информационной безопасности,<br>-основные нормативные правовые акты в области обеспечения информационной безопасности<br>- нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>Владеть<br>-навыками работы с нормативными правовыми актами<br>ПК-2 способностью создавать и исследовать модели | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | автоматизированных систем<br>Знать<br>- основные принципы моделирования и виды моделей, требования, предъявляемые к моделям;<br>- методы оценки качества моделей, методы и средства моделирования;<br>- методы исследования моделей автоматизированных систем;<br>- структуру и состав автоматизированных систем управления<br>Уметь<br>- применять различные методы моделирования автоматизированных систем;<br>- выбирать методы и средства моделирования подсистем защиты информации;<br>- анализировать и оценивать угрозы информационной безопасности объекта.<br>Владеть<br>- навыками анализа информационной инфраструктуры автоматизированной системы;<br>- методами моделирования автоматизированных систем;<br>- основами построения моделей автоматизированных систем;<br>- навыками формализации задач и постановки задач моделирования;<br>- навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.<br>ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Знать<br>-Базовую модель угроз ПДн<br>-Нормативно-методические документы в области моделирования угроз<br>-Способы реализации угроз безопасности информации<br>-Типы нарушителя информационной безопасности в автоматизированных системах<br>-Методику разработки модели угроз<br>Уметь<br>-Разрабатывать частную модель угроз автоматизированной системы<br>-Определять актуальные угрозы для автоматизированной системы;<br>-Разрабатывать модель нарушителя информационной безопасности автоматизированных систем информационно-технологических ресурсов автоматизированных систем.<br>Владеть<br>- Навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите;<br>- Навыками разработки частных моделей угроз | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы<br>Знать<br>- методологию анализа рисков информационной безопасности;<br>- методики определения информационно-технологических ресурсов, подлежащих защите;<br>Уметь<br>- выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите.<br>-оценить риски информационной безопасности автоматизированной системы<br>Владеть<br>- навыками анализа рисков информационной безопасности автоматизированных систем<br>-методиками анализа рисков<br>ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>─ источники и классификацию угроз информационной безопасности;<br>─ основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;<br>─ основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;<br>Уметь<br>─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;<br>─ классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;<br>─определять параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения<br>поддерживать конфигурацию информационной системы и ее системы защиты информации<br>Владеть<br>─ навыками документирования действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ методами формирования требований по защите информации;<br>─ навыками анализа основных узлов и устройств современных автоматизированных систем;<br>─ навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем<br>─ навыками обеспечения защиты информации при выводе из эксплуатации аттестованной информационной системы<br>ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем<br>Знать<br>─ методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ современную нормативно-правовую базу создания защищенных распределенных информационных систем;<br>─ инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей<br>Уметь<br>─ разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;<br>─ применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем<br>Владеть<br>─ методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем;<br>─ навыками разработки комплексной инфраструктуры защищенной информационной системы;<br>─ навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации<br>ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности<br>Знать<br>- Понятия функциональной и системной архитектуры информационных систем, ядра безопасности информационных систем<br>- Основные принципы построения защищенных распределенных компьютерных систем<br>- Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах.<br>- Современные принципы построения архитектуры ИС.<br>Уметь<br>- Осуществлять анализ несложных процессов проектирования;<br>- Применять отечественные и зарубежные стандарты в области | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | компьютерной безопасности для проектирования средств защиты информации компьютерной системы<br>- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов<br>Владеть<br>- Способами определения уровней защищенности и доверия программно-аппаратных средств защиты информации<br>- Практическими навыками определения уровня защищенности и доверия программно-аппаратных средств защиты информации<br>- Определять уровни защищенности и доверия программно-аппаратных средств защиты информации • Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем<br>- Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации<br>- Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем;<br>- Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах<br>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<br>Знать<br>- Современные технологии программирования.<br>- Основные виды интегрированных сред разработки программного обеспечения.<br>- Современные технологии и методы программирования, предназначенные для создания прикладных программ в защищенном исполнении.<br>- Принципы работы элементов и функциональных узлов электронной аппаратуры;<br>-Типовые схемотехнические решения основных узлов и блоков электронной аппаратуры<br>- Принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ;<br>Уметь<br>- Реализовывать на языке высокого уровня алгоритмы решения профессиональных задач;<br>- Работать с основными средами интегрированной разработки | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | программного обеспечения;<br>- Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;<br>- Реализовывать разработанную структуру классов для задач предметной области.<br>-Работать с современной элементной базой электронной аппаратуры;<br>-Использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации<br>- Разрабатывать топологию вычислительной сети в соответствии с требованиями технического задания.<br>Владеть<br>- Навыками реализации алгоритмов на языках программирования высокого уровня;<br>- Навыками пользования библиотеками прикладных программ для решения прикладных задач профессиональной области.<br>- Способностью использовать языки, системы и инструментальные средства разработки автоматизированных систем.<br>-Навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации;<br>- Методиками проектирования топологии вычислительных сетей;<br>- Навыками настройки сетевого оборудования.<br>ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- особенности решений по ЗИ в информационных процессах и системах;<br>- определения рисков ИБ применительно к ОИ с заданными характеристиками;<br>- методы и подходы к реализации системы управления безопасностью АИС;<br>- методы анализа процессов для определения актуальных угроз<br>Уметь<br>- оценивать различные инструменты в области проектирования и управления ИБ;<br>- разрабатывать политики безопасности информации АС;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.<br>Владеть<br>- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | управления рисками ИБ.<br>ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы<br>Знать<br>- способы организации обмена данными при помощи технологий RPC,RMC и очередей;<br>- криптографические протоколы обмена информацией;<br>- общий порядок действий по выбору мер защиты информации для их реализации в информационной системе<br>- методы проектирования средств защиты информации;<br>Уметь<br>- разрабатывать программное обеспечение по технологии Socket с учетом возможных состояний передающей, приемной сторон и линии связи;<br>- разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средства защиты информации АС<br>- выбрать меры защиты информации для их реализации в информационной системе в рамках ее системы защиты информации<br>Владеть<br>- навыками оформления программной документации по ЕСПД;<br>- методами исследования информационно-технологических ресурсов<br>-навыками определения необходимого набора мер защиты информации (базового, адаптированного, уточненного)<br>ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации<br>Знать<br>- Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.<br>- Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.<br>- Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.<br>Уметь<br>- Участвовать в настройке технических средств обеспечения информационной безопасности.<br>- Самостоятельно настраивать технические средства обеспечения информационной безопасности.<br>- Исследовать эффективность контрольных проверок | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | работоспособности применяемых технических средств защиты информации.<br>- Применять технические средства обеспечения информационной безопасности.<br>- Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ.<br>- Применять программные и программно-аппаратные средства обеспечения ИБ.<br>Владеть<br>- Техникой настройки технических средств обеспечения информационной безопасности<br>- Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем.<br>- Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.<br>- Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.<br>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем<br>Знать<br>-уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий;<br>- положение о системе сертификации средств защиты информации;<br>-продукцию, которую необходимо сертифицировать;<br>-состав участников системы сертификации и их основные функции;<br>-этапы сертификации;<br>- требования к проведению испытаний СЗИ;<br>-порядок проведения сертификационных испытаний<br>Уметь<br>─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия;<br>─ проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия<br>─ проводить анализ сертификата соответствия.<br>Владеть<br>─ нормативно-правовой базой в области сертификации средств защиты информации<br>─навыками проведения испытаний средств защиты информации<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | систем с учетом нормативных документов по защите информации<br>Знать<br>─ Средства анализа информационной безопасности;<br>─ Классификацию систем защиты информации;<br>─ Средства организации аттестации по требованиям безопасности информации<br>Уметь<br>─ Принимать участие в аттестационных испытаниях системы защиты информации и анализе результатов;<br>─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований по обеспечению информационной безопасности.<br>Владеть<br>─ Навыками использования средств анализа информационной безопасности;<br>─ Навыками проведения аттестации в соответствии с существующими нормативами.<br>ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации<br>Знать<br>- перечень инструментов для проведения мониторинга защищенности информации;<br>- базовый функционал инструментов для проведения мониторинга защищенности информации;<br>Уметь<br>- применять технические средства для проведения мониторинга беспроводных сетей;<br>- применять технические средства для проведения мониторинга проводных сетей построенных на основе неуправляемых коммутаторов;<br>Владеть<br>- навыками работы с специализированным программным обеспечением для проведения мониторинга защищенности информации в автоматизированной системе;<br>ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности<br>Знать<br>-организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации<br>-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 | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | сертификации средств защиты информации;<br>Уметь<br>-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>-анализировать и обобщения информации на стадии принятия и реализации управленческого решения,<br>-пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров<br>Владеть<br>-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований,<br>-методами организации и управления деятельностью служб защиты информации на предприятии<br>-навыками организации и обеспечения режима секретности<br>-навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов<br>ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы<br>Знать<br>- нормативные методические документы ФСТЭК России в области ИБ;<br>- основные принципы создания системы управления информационной безопасностью.<br>- методы реализации системы управления безопасностью<br>Уметь<br>- проводить оценку информационных рисков,<br>- обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности;<br>- расследовать инциденты ИБ;<br>- разрабатывать предложения по совершенствованию СУИБ АС.<br>Владеть<br>- навыками расчета и управления рисками ИБ;<br>- навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.<br>- навыками подготовки документации СУИБ<br>ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- Основы организационного и правового обеспечения ИБ. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Основные нормативные и правовые акты в области обеспечения ИБ.<br>- Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области ЗИ.<br>- классификацию информационных систем по требованиям защиты информации.<br>Уметь<br>- Определять класс защищенности информационной системы<br>- Принимать участие в реализации разработанной АС с учетом требований информационной безопасности.<br>- Готовить сопроводительную документацию к разработанной АС в защищенном исполнении.<br>- Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении.<br>- выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы<br>- определять виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации<br>Владеть<br>- Навыками разработки автоматизированных систему с учетом требований ИБ.<br>- Навыками контроля разработки АС с учетом требований ИБ.<br>- Навыками выбора средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации<br>- Навыками разработки сопроводительной документации к разработанной подсистеме защиты информации АС<br>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем<br>Знать<br>─ нормативные требования по защите информации; критерии оценки защищенности АС; способы анализа и оценке угроз информационной безопасности;<br>─ 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;<br>Уметь<br>─ применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;<br>─ разрабатывать, реализовывать, оценивать и корректировать | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | процессы менеджмента информационной безопасности;<br>─ разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем<br>Владеть<br>─ навыками администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;<br>─ нормативными требованиями по защите информации;<br>─ навыками организации и обеспечения режима секретности<br>─ навыками разработки организационно-распорядительных документов<br>ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации<br>Знать<br>- основные угрозы безопасности информации и модели нарушителя ОИ;<br>- принципы формирования политики информационной безопасности организации.<br>- способы контроля эффективности реализации политики информационной безопаности<br>Уметь<br>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- разрабатывать частные политики ИБ АС;<br>- контролировать эффективность принятых мер по реализации частных политик ИБ АС.<br>Владеть<br>- навыками разработки политик безопасности различных уровней.<br>- навыками и методами контроля эффективности сформированной политики информационной безопасности<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа<br>Знать<br>- Методы формирования требований по защите информации ограниченного доступа<br>- Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.<br>- Организационные меры по защите информации ограниченного доступа<br>Уметь<br>- Использовать методы формирования требований по защите информации ограниченного доступа<br>- Классифицировать средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации ограниченного доступа<br>Владеть<br>- Методами формирования требований по защите информации ограниченного доступа<br>- Навыками анализа методов формирования требований по защите информации ограниченного доступа<br>ПК-24 способностью обеспечить эффективное применение информационно- технологических ресурсов автоматизированной системы с учетом требований информационной безопасности<br>Знать<br>- методы повышения уровня безопасности за счет настройки прав доступа к ресурсам автоматизированной системы;<br>Уметь<br>- применять меры организационного и программно-технического уровня, направленных на защиту информационно-технологических ресурсов автоматизированной системы<br>- выявлять узлы автоматизированной системы, не обеспечивающие требуемый уровень защиты информации<br>Владеть<br>- навыками определения возможных векторов атаки на автоматизированную систему и осуществлять выбор средств защиты информации;<br>ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций<br>Знать<br>- Принципы администрирования баз данных. Средства обеспечения безопасности данных.<br>- Организацию защиты информации баз данных. Сравнительный анализ эффективности применения средств обеспечения безопасности данных<br>Уметь<br>- Анализировать работоспособность базы данных.<br>- Принимать участие в настройке средств обеспечения безопасности данных, обрабатываемых в СУБД. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Самостоятельно применять средства обеспечения безопасности данных.<br>- Участвовать в восстановлении работоспособности систем баз данных при возникновении нештатных ситуаций.<br>- Организовывать безопасность систем баз данных<br>- Выявлять инциденты и реагировать на них<br>- Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации<br>Владеть<br>- Основными средствами обеспечения безопасности данных.<br>- Навыками работы с нормативными документами по администрированию баз данных.<br>- Средствами обеспечения безопасности данных.<br>- Навыками разработки и администрирования базы данных.<br>- Навыками организации безопасности систем баз данных.<br>- Средствами обеспечения безопасности данных и АИС.<br>- Навыками сопровождения функционирования системы защиты информации информационной системы в ходе ее эксплуатации<br>- Навыками анализа инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий<br>ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы<br>Знать<br>─ Основные принципы работы системы информационной безопасности автоматизированной системы и всех ее подсистем;<br>─ Принципы администрирования системы информационной безопасности автоматизированной системы.<br>Уметь<br>─ Настраивать систему информационной безопасности автоматизированной системы;<br>─ Настраивать подсистемы системы информационной безопасности автоматизированной системы;<br>─ Самостоятельно администрировать систему информационной безопасности автоматизированной системы.<br>Владеть<br>─ Навыками работы с системой информационной безопасности автоматизированной системы;<br>─ Навыками работы с подсистемами системы информационной безопасности автоматизированной системы;<br>─ Навыками администрирования системы информационной безопасности автоматизированной системы.<br>ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | безопасности автоматизированной системы<br>Знать<br>─ Способы обработки исключительных ситуаций<br>─ Нормативные документы по стандартизации и сертификации программной защиты.<br>─ Цели и задачи разработки политики информационной безопасности<br>─ Методы и средства анализа достаточности мер по обеспечению ИБ ПО<br>─Порядок контроля (мониторинга) за обеспечением уровня защищенности информации<br>Уметь<br>─ Разрабатывать порядок эксплуатации программного обеспечения<br>─ Разрабатывать политику учетных записей для эксплуатации информации ресурсов и программного обеспечения<br>─ Проводить мониторинг и аудит защищенности ПО<br>─Осуществлять контроль за событиями безопасности и действиями пользователей в информационной системе<br>Владеть<br>─ Методами анализа достаточности мер по обеспечению ИБ процессов создания и эксплуатации ПО<br>─ Методами контроля соблюдения политики учетных записей<br>─ Навыками регламентации обслуживания и осуществления модификации программного обеспечения<br>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<br>Знать<br>- Основы построения систем обработки и передачи информации, их современное состояние развития.<br>-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<br>- Особенности обработки информации с использованием компьютерных систем<br>Уметь<br>- Проводить поиск, обобщение и систематизацию современной научно -технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>- Анализировать современную научно-техническую информацию по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>Владеть | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | - Навыками сбора современной научно-технической информации по рассматриваемым в рамках учебной-практики проблемам и задачам.<br>- Навыками проведения исследовательских работ по рассматриваемым в рамках учебной-практики проблемам и задачам<br>ПК-3 способностью проводить анализ защищенности автоматизированных систем<br>Знать<br>- Критерии оценки эффективности и надежности средств защиты распределенных информационных систем<br>- Принципы построения и функционирования распределенных информационных систем в защищённом исполнении<br>-Мероприятия для обеспечения защиты информации<br>Уметь<br>-Анализировать техническую и сопроводительную документацию по обеспечению ИБ.<br>-Анализировать целесообразность выбора технических, программно–аппаратных и криптографических компонентов автоматизированных систем с целью совершенствования защиты.<br>-Проводить контроль за событиями безопасности и действиями пользователей в информационной системе<br>-Проводить анализ и оценку функционирования системы защиты информации информационной системы<br>Владеть<br>-Навыками выбора средств защиты информации<br>-Навыками документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе<br>ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ<br>Знать<br>-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов<br>Уметь<br>-принимать участие в разработке проектов нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;<br>- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности<br>Владеть<br>-навыками разработки научно-техническую документации, научно-технических отчетов по результатом выполненных работ | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы<br>Знать<br>- систему организационных мер, направленных на защиту информации ограниченного доступа<br>- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;<br>- уровни политик информационной безопасности назначение политик верхнего, среднего и нижнего уровня<br>Уметь<br>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;<br>-разрабатывать политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала<br>Владеть<br>- владеть навыками разработки политик безопасности различных уровней.<br>-владеть навыками формирования комплекта организационной документации, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации<br>ПК-28 способностью управлять информационной безопасностью автоматизированной системы<br>Знать<br>-методы и средства контроля охраняемых сведений<br>- программные средства, поддерживающие управление информационной безопасностью<br>-отечественный и зарубежный опыт в области управления информационной безопасностью<br>- основные принципы создания системы управления информационной безопасностью<br>Уметь<br>-разрабатывать политики безопасности для элементов системы ОУ<br>-расследовать инциденты ИБ<br>-разрабатывать комплекс мероприятий по предотвращению инцидентов ИБ<br>-готовить предложения для актуализации организационных мер по защите информационных систем<br>- разрабатывать профили защиты<br>Владеть<br>- терминологией и процессным подходом построения СУИБ.<br>-навыками определения актуальных угроз и применения мер их | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | нейтрализации<br>- навыками составления технических политик безопасности<br>**Практика включает в себя следующие разделы**:<br>1. Подготовительный (ознакомительный)<br>2. Экспериментально- исследовательский<br>3. Обработка и анализ полученной информации.<br>4. Отчетный | |
| **Б3** | **Государственная итоговая аттестация** | |
| **Б3. Б.01** | **Подготовка к сдаче и сдача государственного экзамена**<br>Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.<br>В соответствии с видами и задачами профессиональной деятельности выпускник на государственной итоговой аттестации должен показать соответствующий уровень освоения следующих компетенций:<br>– способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);<br>– способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);<br>– 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);<br>– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);<br>– 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);<br>– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);<br>– 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);<br>– способностью к самоорганизации и самообразованию (ОК-8);<br>– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9). | *Общая трудоемкость дисциплины составляет 3 зачетных единицы* ***108*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);<br>– 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);<br>– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);<br>– способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);<br>– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);<br>– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);<br>– способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);<br>– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).<br>– 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);<br>– способностью создавать и исследовать модели автоматизированных систем (ПК-2);<br>– способностью проводить анализ защищенности автоматизированных систем (ПК-3);<br>– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);<br>– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);<br>– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6); | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);<br>– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);<br>– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);<br>– 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);<br>– способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);<br>– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);<br>– способностью участвовать в проектировании средств защиты информации автоматизированной Системы (ПК-13);<br>– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);<br>– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);<br>– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);<br>– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);<br>– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);<br>– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);<br>– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);<br>– способностью разрабатывать проекты документов, | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);<br>– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);<br>– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);<br>– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);<br>– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);<br>– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);<br>– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);<br>– способностью управлять информационной безопасностью автоматизированной системы (ПК-28).<br><br>– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);<br>– способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);<br>– способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);<br>– способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);<br>– способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5); | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Государственный экзамен проводится в два этапа:<br>• на первом этапе проверяется сформированность общекультурных компетенций;<br>• на втором этапе проверяется сформированность общепрофессиональных и профессиональных компетенций в соответствии с учебным планом.<br>Первый этап государственного экзамена проводится в форме компьютерного тестирования.<br><br>Ко второму этапу государственного экзамена допускается обучающийся, получивший оценку «зачтено» на первом этапе.<br>Второй этап государственного экзамена проводится в письменной форме.<br>Второй этап государственного экзамена включает 3 теоретических вопроса и 1 практическое задание.<br>Обучающийся, успешно сдавший государственный экзамен, допускается к выполнению и защите выпускной квалификационной работы. | |
| **Б3.Б.02** | **Подготовка к защите и защита выпускной квалификационной работы**<br><br>Государственная итоговая аттестация проводится государственными экзаменационными комиссиями в целях определения соответствия результатов освоения обучающимися образовательных программ соответствующим требованиям федерального государственного образовательного стандарта.<br><br>В соответствии с видами и задачами профессиональной деятельности выпускник на государственной итоговой аттестации должен показать соответствующий уровень освоения следующих компетенций:<br>– способностью использовать основы философских знаний для формирования миро-воззренческой позиции (ОК-1);<br>– способностью использовать основы экономических знаний в различных сферах де-ятельности (ОК-2);<br>– 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);<br>– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);<br>– способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, | *Общая трудоемкость дисциплины составляет 6 зачетных единиц* ***216*** *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | общества и государства, соблюдать нормы профессиональной этики (ОК-5);<br>– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);<br>– 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);<br>– способностью к самоорганизации и самообразованию (ОК-8);<br>– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).<br><br>– способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);<br>– 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);<br>– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);<br>– способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах (ОПК-4);<br>– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);<br>– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);<br>– способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);<br>– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).<br><br>– 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 |
| | в том числе на иностранном языке (ПК-1);<br>– способностью создавать и исследовать модели автоматизированных систем (ПК-2);<br>– способностью проводить анализ защищенности автоматизированных систем (ПК-3);<br>– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);<br>– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);<br>– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере про-фессиональной деятельности (ПК-6);<br>– способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);<br>– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);<br>– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);<br>– способностью применять знания в области электроники и схемотехники, техноло-гий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизиро-ванных систем в сфере профессиональной деятельности (ПК-10);<br>– способностью разрабатывать политику информационной безопасности автомати-зированной системы (ПК-11);<br>– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);<br>– способностью участвовать в проектировании средств защиты информации автома-тизированной Системы (ПК-13);<br>– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты ин-формации (ПК-14);<br>– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);<br>– 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 |
| | (ПК-16);<br>– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);<br>– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);<br>– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);<br>– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);<br>– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);<br>– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);<br>– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);<br>– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);<br>– способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);<br>– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);<br>– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);<br>– способностью управлять информационной безопасностью автоматизированной системы (ПК-28).<br><br>– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1); | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | – способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);<br>– способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);<br>– способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);<br>– способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);<br>Выполнение и защита выпускной квалификационной работы является одной из форм государственной итоговой аттестации.<br>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.<br>Обучающий, выполняющий выпускную квалификационную работу должен показать свою способность и умение:<br>– определять и формулировать проблему исследования с учетом ее актуальности;<br>– ставить цели исследования и определять задачи, необходимые для их достижения;<br>– анализировать и обобщать теоретический и эмпирический материал по теме исследования, выявлять противоречия, делать выводы;<br>– применять теоретические знания при решении практических задач;<br>– делать заключение по теме исследования, обозначать перспективы дальнейшего изучения исследуемого вопроса;<br>– оформлять работу в соответствии с установленными требованиями;<br><br>Защита выпускной квалификационной работы проводится на заседании государственной экзаменационной комиссии и является публичной.<br>**Примерный перечень тем выпускных квалификационных работ**<br><br>1. Аудит защищенности информационных ресурсов предприятия. | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | 2. Разработка системы защиты корпоративной сети учебного заведения на основе технологии VipNet.<br>3. Разработка системы криптографической защиты облачного хранилища данных<br>4. Разработка средства моделирования угроз безопасности информационной системы на основе теории графов.<br>5. Разработка автоматизированного комплекса для оценки защищенности от утечки по акустическим каналам.<br>6. Разработка защищенной информационной системы персональных данных.<br>7. Разработка автоматизированной системы контроля управления доступом.<br>8. Разработка защищенной корпоративной сети для топливной компании с применением технологии VPN.<br>9. Разработка системы защиты для ИСПДн, подключенной к ГИС. | |
| **ФТД** | **Факультативы** | |
| **ФТД.01** | **Тестирование систем защиты информации автоматизированных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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 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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы** | *Общая трудоемкость дисциплины составляет **1** зачетных единицы **36** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Дисциплина Тестирование систем защиты информации автоматизированных систем 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 Сети и системы передачи информации Программно-аппаратные средства обеспечения информационной безопасности Безопасность систем баз данных Безопасность сетей ЭВМ Знания (умения,владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик: Анализ уязвимостей программного обеспечения Защита электронного документооборота Методы и стандарты оценки защищенности компьютерных систем Методы мониторинга информационной безопасности АС Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности Методы проектирования систем защиты распределенных информационных систем Обеспечение информационной безопасности критической информационной инфраструктурой<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Тестирование систем защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем<br>Знать<br>─ правила оформления научно-технической документации;<br>─ принципы работы и параметры используемого оборудования для проведения экспериментально-исследовательских работ;<br>─ типовые схемы экспериментального исследования основных электронных приборов и устройств<br>Уметь<br>─ составлять заявку на сертификацию средств защиты информации/продление срока действия сертификата соответствия;<br>─ проводить анализ решения о проведении сертификации средства защиты информации /сертификационных испытаний для продления срока действия сертификата соответствия<br>─ проводить анализ сертификата соответствия.<br>Владеть<br>─ терминологий в области экспериментально–исследовательских работ, а также способностью вести аргументированную дискуссию по результатам экспери-ментально-исследовательских работ; | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ нормативно-правовой базой в области сертификации средств защиты информации<br>ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>Знать<br>─ Средства анализа информационной безопасности;<br>─ Классификацию систем защиты информации;<br>─ Средства организации аттестации ВП по требованиям безопасности информации.<br>Уметь<br>─ Принимать участие в исследованиях аттестации системы защиты информации;<br>─ Принимать участие в исследованиях и анализе аттестации системы защиты информации;<br>─ Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.<br>Владеть<br>─ Навыками использования средств анализа информационной безопасности;<br>─ Навыками проведении экспериментально-исследовательских работ при аттестации АС с учетом требований к обеспечению информационной безопасности;<br>─ Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.<br>**Дисциплина включает в себя следующие разделы:**<br>1.Сертификация средств защиты информации автоматизированных систем<br>1.1 Общие сведения. Организационная структура системы сертификации. Подача заявки на сертификацию<br>1.2 Принятие решения о проведении сертификации средства защиты информации. Сертификационные испытания средства защиты информации<br>1.3 Оформление экспертного заключения по результатам сертификации средства<br>защиты информации и проекта сертификата соответствия. Маркирование средств защиты информации. Внесение изменений в сертифицированное средство защиты информации. Переоформление, продление, приостановление и прекращение сертификата<br>2. Аттестации автоматизированных систем с учетом нормативных документов по защите информации<br>2.1 Общие положения. Организационная структура системы | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | аттестации<br>2.2 Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте. Порядок проведения аттестации и контроля<br>2.3 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации. | |
| **ФТД.02** | **Разработка эксплуатационной документации на системы защиты информации автоматизированных систем**<br>**1 Цели освоения дисциплины (модуля)**<br>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.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Разработка эксплуатационной документации на системы защиты информации автоматизированных систем входит в вариативную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Безопасность операционных систем<br>Сети и системы передачи информации<br>Безопасность сетей ЭВМ<br>Безопасность систем баз данных<br>Программно-аппаратные средства обеспечения информационной безопасности<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Управление информационной безопасностью<br>Информационная безопасность систем организационного управления<br>Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности<br>Производственная-преддипломная практика<br>Методы проектирования систем защиты распределенных информационных систем | *Общая трудоемкость дисциплины составляет **1** зачетных единицы **36** акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Обеспечение информационной безопасности критической информационной инфраструктурой<br>Производственная-преддипломная практика<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Разработка эксплуатационной документации на системы защиты информации автоматизированных систем» обучающийся должен обладать следующими компетенциями:<br>ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа<br>Знать<br>─ основные меры по защите информации в автоматизированных системах;<br>─ особенности защиты информации в автоматизированных системах управления технологическими процессами;<br>─ угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах.<br>Уметь<br>─ определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах;<br>─ Оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.<br>Владеть<br>─ методами анализа защищенности информационной инфраструктуры автоматизированной системы;<br>─ навыками формирования требований по защите информации, включая использование математического аппарата для решения прикладных задач;<br>ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем<br>Знать<br>─ руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;<br>─ нормативные правовые акты в области защиты информации;<br>─ основные методы управления проектами в области информационной безопасности.<br>Уметь | |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | ─ разрабатывать эксплуатационную документацию на систему защиты автоматизированных систем;<br>─ анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем;<br>─ проводить технико-экономическое обоснование и исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.<br>Владеть<br>─ методами анализа технической документации информационной инфраструктуры автоматизированной системы;<br>─ навыком документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.<br>**Дисциплина включает в себя следующие разделы:**<br>1. Техническая документация автоматизированных систем в защищенном исполнении<br>1.1 Общие сведения. Назначение технической документации. Требования к технической документации<br>1.2 Стандарты в области информационных систем. Комплекс стандартов и руководящих документов на автоматизированные системы<br>1.3 Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении.<br>2. Разработка эксплуатационной документации<br>2.1 Общие положения. Состав эксплуатационной документации. Виды и номенклатура эксплуатационных документов. Требования к эксплуатационной документации<br>2.2 Составление руководства пользователя с выделением действий по обеспечению информационной безопасности.<br>2.3 Составление программы и методики испытаний системы защиты автоматизированной системы. | |
| **ФТД.03** | **Технологическое предпринимательство**<br>**1 Цели освоения дисциплины (модуля)**<br>Целью освоения дисциплины «Технологическое предпринимательство» является формирование комплексных и систематизированных знаний, а также привитие практических умений и навыков для решения профессиональных задач в сфере ком-мерциализации сложных технологий, организации процесса технологического предпринимательства и управления инновационными проектами.<br>К основным **задачам** курса относятся:<br>- изучение теории функционирования инновационной экономики | *Общая трудоемкость дисциплины составляет **3** зачетных единицы **108*** |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | и технологического предпринимательства;<br>- рассмотрение принципов организации, управления и оценки инновационно-предпринимательской деятельности;<br>- анализ мер государственной поддержки инновационной деятельности и развития инновационной экосистемы;<br>- изучение основ коммерциализации инноваций и развития высокотехнологического бизнеса.<br>- формирование проектной команды;<br>- выбор бизнес-модели и разработка бизнес-плана;<br>- анализ рынка и прогноз продажи, анализ потребительского поведения и рисков развития компании.<br>**2 Место дисциплины (модуля) в структуре образовательной программы**<br>Дисциплина Технологическое предпринимательство входит в обязательную часть учебного плана образовательной программы.<br>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:<br>Экономика<br>Продвижение научной продукции<br>Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:<br>Производственная-преддипломная практика<br>Подготовка к защите и защита выпускной квалификационной работы<br>**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**<br>В результате освоения дисциплины (модуля) «Технологическое предпринимательство» обучающийся должен обладать следующими компетенциями:<br>ОК-2 - способностью использовать основы экономических знаний в различных сферах деятельности<br>Знать<br>основы экономических знаний, составляющих категориальный аппарат технологического предпринимательства, специфику и возможности их применения в различных сферах профессиональной деятельности;<br>Уметь<br>оперировать основами экономических знаний, составляющих категориальный аппарат технологического предпринимательства;<br>использовать основы экономических знаний, составляющих категориальный аппарат технологического предпринимательства в различных сферах профессиональной деятельности; | *акад. часов* |

| Индекс | Наименование дисциплины | Общая трудоемкость, акад. часов (ЗЕТ) |
|---|---|---|
| 1 | 2 | 3 |
| | Владеть<br>профессиональным языком предметной области знания;<br>категориальным аппаратом технологического предпринимательства в различных сферах деятельности;<br>ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности<br>Знать<br>правовые основы технологического предпринимательства;<br>Уметь<br>понимать и отбирать нормативные документы и методические материалы, необходимые для коммерциализации сложных технологий, технологического предпринимательства и управления инновационными проектами, применять их в процессе деятельности<br>Владеть<br>идентификацией корректных нормативных документов и методических материалов, регулирующих процессы коммерциализации сложных технологий, технологического предпринимательства и управления инновационными проектами и применять их в деятельности<br>ОК-8 - способностью к самоорганизации и самообразованию<br>Знать<br>особенности организации процесса деятельности в технологическом предпринимательстве, основы самоорганизации и самообразования необходимые для управления инновационными проектами в процессе технологического предпринимательства;<br>Уметь<br>ставить цели профессионально-личностного развития при решении задач в сфере коммерциализации сложных технологий, организации процесса технологического предпринимательства и управления инновационными проектами с учётом индивидуально-личностных особенностей, возможностей самоорганизации и самообразования;<br>Владеть<br>методами и технологиями постановки целей профессионально-личностного развития и их реализации, критической оценки результатов самоорганизации, самообразования при решении задач в сфере коммерциализации сложных технологий, организации процесса технологического предпринимательства и управления инновационными проектами<br><br>**Дисциплина включает в себя следующие разделы:**<br>Раздел 1.<br>Введение в технологическое предпринимательство<br>1.1 Сущность и свойства инноваций. Классификация инноваций | |

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