

## АННОТАЦИИ ДИСЦИПЛИН ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

### 10.05.03 Информационная безопасность автоматизированных систем

#### Специализация Обеспечение информационной безопасности распределенных информационных систем

Индекс	Наименование дисциплины	Общая трудоем- кость, Часов (зет)
1	2	3
Б1	<b>ДИСЦИПЛИНЫ (МОДУЛИ)</b>	
Б1.Б	<b>БАЗОВАЯ ЧАСТЬ</b>	
Б1.Б.1	<p style="text-align: center;"><b>ИСТОРИЯ</b></p> <p><b>Цель изучения дисциплины:</b> Сформировать у студентов комплексное представление о культурно-историческом своеобразии России, ее месте в мировой и европейской цивилизации, дать знания по истории России, научить их анализировать и систематизировать исторический материал на основе различных методологических принципов и подходов, сформировать историческое мировоззрение, базирующееся на патриотизме и уважении к историческим ценностям других народов и государств.</p> <p>Сформировать систематизированные знания об основных закономерностях и особенностях всемирно-исторического процесса, с акцентом на изучение истории России; введение в круг исторических проблем, связанных с областью будущей профессиональной деятельности, выработка навыков получения, анализа и обобщения исторической информации.</p> <p><b>Задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>- изучение важнейших характеристик исторических периодов в развитии России;</li> <li>- осмысление специфики исторического развития России в условиях взаимодействия и взаимообогащения с другими цивилизациями;</li> <li>- формирование навыков работы с историческими документами, культуры научного изучения исторического материала.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b> Для освоения этого курса необходимо знание предметов «История России», «Всеобщая история» и «Обществознание» (школьный курс). Курс «История Отечества» готовит студента к углублённому восприятию дисциплин «Философия», «Культурология». Знание истории научит студентов самостоятельно давать оценку событий, сформирует их собственную гражданскую позицию, поможет понять и осмыслить важнейшие проблемы современности.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-3</b> способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма</p> <p><b>В результате изучения дисциплины студент должен:</b></p>	<b>144 (4)</b>

**знать:**

- основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире;
- гражданские и личные экономические, культурные, социальные права;
- основы конституционного строя РФ;
- уровни государственной власти в РФ, федеративное устройство РФ;
- полномочия и порядок формирования высших органов власти основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в российской федерации;
- методы социальных наук;
- исторические факты и события истории России в хронологической последовательности;
- базовые исторические термины и понятия;
- осознавать место истории России во всемирно-историческом процессе;
- современные версии и трактовки важнейших проблем отечественной и всемирной истории;
- основные этапы и закономерности исторического процесса;
- исторических и общественных деятелей отечественной истории;
- модели политической организации власти на разных этапах истории России;
- движущие силы исторического процесса.

**уметь:**

- анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности;
- определять собственную позицию по отношению к явлениям современной жизни, исходя из их исторической обусловленности;
- устанавливать причинно-следственные связи между явлениями;
- определять собственную позицию по отношению к явлениям современной жизни, исходя из их исторической обусловленности;
- применять основные законы гуманитарных и социальных наук в профессиональной деятельности;
- применять знания прав и свобод гражданина РФ в практической деятельности;
- действовать на основе права в соответствии гражданским долгом;
- анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности;
- проявлять уважительное и бережное отношение к историческому наследию и культурным традициям, образу жизни, поведению, чувствам, мнениям, идеям, верованиям и обычаям членов профессионального коллектива и окружающей социальной среды;
- проводить исторический анализ событий, анализировать и оценивать социальную информацию;
- всесторонне объективно оценивать и обобщать исторические факты и события;
- использовать в практической деятельности исторические знания;
- применять понятийно-категориальный аппарат при изложении фактов и явлений истории;

**владеть навыками:**

- использовать навыки исторического анализа при критическом восприятии получаемой извне социальной информации;
- навыками выбора, обоснования, реализации правовой информации в профессиональной деятельности;
- навыками различать в исторической информации факты и мнения, исторические описания и исторические объяснения;
- навыками анализировать исторические события и явления, исторические источники;

	<p>- сопоставлять различные версии и оценки исторических событий и личностей, определять собственное отношение к дискуссионным проблемам прошлого и современности.</p> <p><b>Дисциплина включает в себя следующие разделы:</b> Теория и методология исторической науки. Исследователь и исторический источник. Особенности становления государственности в России Русские земли в XIII-XV вв. Россия в XVI – XVII вв. в контексте развития европейской цивилизации. Россия в XVIII-XIX вв. Попытки модернизации и промышленный переворот. Россия и мир в XX веке. Раздел 8. Россия в XXI веке.</p>	
<p><b>Б1.Б.2</b></p>	<p style="text-align: center;"><b>ИНОСТРАННЫЙ ЯЗЫК</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины « Иностранный язык » являются: повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования (средняя школа), и овладение студентами необходимым и достаточным уровнем коммуникативной компетенции для решения социально-коммуникативных задач в различных областях бытовой, культурной, профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.</p> <p><b>Место дисциплины в структуре ООП:</b> Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате обучения в средней школе. Знания (умения, навыки), полученные при изучении данной дисциплины, будут необходимы для изучения дисциплины «Иностранный язык в профессиональной деятельности» и дисциплин профессионального цикла, использующих терминологию иностранных языков, и позволят студентам интегрироваться в международную профессиональную среду и использовать иностранный язык как средство межкультурного и профессионального общения.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-7</b> 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 <b>ПК-1</b> способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</p> <p><b>В результате изучения дисциплины студент должен:</b> <b>Знать:</b> - лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке; - структуру и основы построения основных жанров письменных и устных текстов социально – бытовой и академической тематик; - иностранный язык в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке; - правила речевого этикета в соответствии с ситуациями межкультурного общения в зависимости от стиля и характера общения в социально-бытовой и академической сферах; <b>Уметь:</b> - читать и переводить научно-техническую литературу на иностранном языке</p>	<p><b>252 (7)</b></p>

	<p>по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи;          монологическую и диалогическую речь на бытовые и специальные темы;          -владеть всеми видами чтения адаптированной литературы;          - фиксировать информацию, получаемую при чтении текстов;  <b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке;</li> <li>публичной речью (делать сообщения, доклады с предварительной подготовкой);</li> <li>- навыками ведения дискуссии по знакомой проблеме, обоснования и отстаивания своей точки зрения;</li> <li>- навыками общения в области профессиональной деятельности на иностранном языке</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>          Бытовая сфера общения.. Образование в России и за рубежом. Система высшего образования в России и за рубежом. Особенности учебного процесса в разных странах. Студенческая жизнь в России и за рубежом (научная, культурная и спортивная). Мой университет. История и традиции моего университета. Известные ученые и выпускники моего университета. Жизнь мегаполиса. Проблемы транспорта. Мой родной город. Ученые. Изобретатели и их изобретения. Социально-культурная сфера общения. Современные города России и стран изучаемого языка. Облик города в различных странах мира. История архитектуры, типы жилищ в России и за рубежом. Страна изучаемого языка. Традиции, обычаи, достопримечательности. Выдающиеся деятели. Музеи. Образ жизни современного человека в России и за рубежом. Транспорт - проблема мегаполисов и пути ее разрешения. Моя Родина - Россия. Природные богатства. Традиции, обычаи, достопримечательности. Выдающиеся деятели. Научно-техническая сфера общения. Экология. Охрана окружающей среды – глобальная проблема человечества. Мир вокруг нас. Информационные технологии XXI века. Достижения науки и техники. Плюсы и минусы всеобщей информатизации общества.</p>	
<p><b>Б1.Б.3</b></p>	<p style="text-align: center;"><b>ФИЛОСОФИЯ</b></p> <p><b>Цели изучения дисциплины:</b></p> <ul style="list-style-type: none"> <li>К сформировать представление о специфике философии как способе познания и духовного освоения мира;</li> <li>К сформировать целостное представление о процессах и явлениях, происходящих в неживой и живой природе и общественной жизни;</li> <li>К привить навыки работы с оригинальными и адаптированными философскими текстами;</li> <li>К сформировать представление о научных, философских и религиозных картинах мироздания, сущности, назначении и смысле жизни человека;</li> <li>К 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;</li> <li>К сформировать представление о ценностных основаниях человеческой деятельности;</li> <li>К определить основания активной жизненной позиции, ввести в круг философских проблем, связанных с областью будущей профессиональной деятельности.</li> </ul>	<p><b>144 (4)</b></p>

**Место дисциплины в структуре ООП:**

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения таких предшествующих дисциплин как «История Отечества», «Культурология и межкультурное взаимодействие». При освоении дисциплины «Философия» студенты должны опираться на знания основ социально-исторического анализа, уметь оперировать общекультурными категориями, прослеживать динамику социально-политического развития.

Знания и умения (владения), полученные студентами при изучении дисциплины «Философия», необходимы для усвоения последующих дисциплин, где требуются: навыки аналитического мышления; знание и понимание законов развития социально значимых проблем и процессов природы, а также для дисциплин, вырабатывающих коммуникативные способности: «Экономика», «Правоведение». Освоение дисциплины «Философия» позволяет усвоить мировоззренческие основания профессиональной деятельности, грамотно подготовиться к учебной практике, к итоговой государственной аттестации и продолжению образования по магистерским программам.

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ОК- 1** способностью использовать основы философских знаний для формирования мировоззренческой позиции

**В результате изучения дисциплины студент должен:****знать:**

- содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук;
- основные этапы развития философской мысли, основную проблематику и структуру философского знания;
- структурообразующие и обобщающие понятия философии и социальных наук;
- основные философские понятия и категории, закономерности развития природы общества и мышления; основы работы с информацией, средства общения и передачи информации

**уметь:**

- использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач;
- анализировать мировоззренческие, социально и лично значимые философские проблемы;
- применять в профессиональной деятельности базовые и профессионально профилированные знания и навыки по основам философии и социологической теории и методам социологического исследования;
- применять методы и средства познания для интеллектуального развития, повышения культурного уровня, профессиональной компетенции.

**владеть:**

- основными методами научного познания;
- навыками философского мышления для выработки системного, целостного взгляда на проблемы общества;
- способностью к коммуникациям деятельности; культурой мышления, способностью к обобщению, восприятию и анализу информации.

**Дисциплина включает в себя следующие разделы:**

Философия, ее место в культуре. Черты философского знания. Мировоззрение. Структура философского мировоззрения. Исторические типы философии. Древневосточная философия. Античная философия. Религиозная философия Средних веков. Философия эпох Возрождения и Просвещения как основание гуманистических переворотов в философии. Философия Нового

	<p>времени. Исторические типы философии. Немецкая классическая философия. Иррационализм и марксизм как предпосылки преодоления классической метафизики. Основные школы неклассической философии. Основные особенности отечественной философии. Онтологические основания мира и атрибутивные свойства субстанции. Понятие бытия. Его структура. Проблема целостности мира. Субстанциональность мира. Проблема изменчивости мира в рамках философского понимания движения. Развитие. Пространство, время. Проблема познания в философии. Концепции истины. Особенности человеческого бытия. Общество как развивающаяся система. Культура и цивилизация. Общество как развивающаяся система.</p>	
<p><b>Б1.Б.4</b></p>	<p style="text-align: center;"><b>ЭКОНОМИКА</b></p> <p><b>Цель изучения дисциплины:</b> Целью освоения дисциплины является формирование у студентов основ экономического мышления, выработка умения аргументировано судить об экономических проблемах, как в народнохозяйственных масштабах, так и в личной повседневной жизни, обретение опыта самостоятельного принятия эффективных экономических решений. Изучение дисциплины направлено на формирование экономических знаний, знаний основных принципов функционирования как экономики в целом, так и отдельных предприятий.</p> <p><b>Место дисциплины в структуре ООП:</b> Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения следующих дисциплин: - История отечества (духовный мир человека на пороге перехода к индустриальному обществу; роль XX века во всемирно-историческом процессе; пути развития России; менталитет, его эволюция и особенности в Западной Европе, России и других регионах мира); - Математический анализ (графики основных элементарных функций; производная и дифференциал; математические методы в целенаправленной деятельности, основные понятия математической статистики; роль математики в исследованиях). Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для дисциплин «Правоведение», «Основы управленческой деятельности».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-2</b> способностью использовать основы экономических знаний в различных сферах деятельности.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов;</li> <li>- основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности);</li> <li>- основные экономические теории и экономические законы, примеры их действия на практике;</li> <li>- основные теоретические методы научных исследований в экономике.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- анализировать экономические показатели деятельности подразделения;</li> <li>- самостоятельно анализировать социально-политическую и экономическую литературу;</li> <li>- анализировать социально значимые явления и процессы экономического характера.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- методами использования экономических законов при решении</li> </ul>	<p><b>108 (3)</b></p>

	<p>профессиональных задач;  - методологией экономических исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.</p> <p><b>Дисциплина включает в себя следующие разделы:</b>  Введение в экономику. Основы анализа спроса, предложения, рыночного равновесия. Эластичность спроса. и предложения Теория потребительского выбора. Теория фирмы. Производственная функция. Издержки производства. Типы рынков Рынок и конкуренция. Определение цены и объёмов производства на монопольном рынке. Рынок факторов производства. Основные макроэкономические показатели. Макроэкономическая нестабильность Безработица. Инфляция. Макроэкономическое равновесие. Совокупный спрос и совокупное предложение. Деньги. Кредитно-денежная политика. Налоги. Фискальная политика. Экономический рост.</p>	
<p><b>Б1.Б.5</b></p>	<p style="text-align: center;"><b>ПРАВОВЕДЕНИЕ</b></p> <p><b>Цели изучения дисциплины:</b>  Целями освоения дисциплины «Правоведение» являются формирование у студентов знаний для правового ориентирования в системе законодательства, определение соотношения юридического содержания норм с реальными событиями общественной жизни, изучение основополагающих правовых понятий.</p> <p><b>Место дисциплины в структуре ООП:</b>  Для изучения дисциплины необходимы знания, сформированные в результате изучения дисциплин: истории отечества, философия.  Знания, умения, навыки, полученные при изучении данной дисциплины, будут необходимы для итоговой государственной аттестации.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОПК-6</b> способностью применять нормативные правовые акты в профессиональной деятельности  <b>ОК-4</b> способностью использовать основы правовых знаний в различных сферах деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации;</li> <li>- основополагающие конституционные понятия, принципы законности и патриотизма;</li> <li>- принципы профессиональной этики;</li> <li>- законодательство в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- использовать в практической деятельности правовые знания;</li> <li>- анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности;</li> <li>- ориентироваться в системе правовых и социальных норм;</li> <li>- юридически правильно квалифицировать обстоятельства профессиональной деятельности;</li> <li>-использовать нормативные и методические материалы в сфере обеспечения информационной безопасности автоматизированных систем.</li> </ul> <p><b>Владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- поиска нормативной правовой информации, необходимой для</li> </ul>	<p><b>144 (4)</b></p>

	<p>профессиональной деятельности;</p> <ul style="list-style-type: none"> <li>- анализа и разрешения юридических вопросов в различных сферах</li> <li>- способами юридического анализа обстоятельств в сфере информационной безопасности;</li> <li>- разработки проектов нормативных и методических материалов в сфере будущей профессиональной деятельности.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Государство и право  Государство. Его роль в жизни общества. Основы конституционного права. Право. Его роль в жизни общества. Права человека и гражданина РФ. Источники российского права. Правонарушение и юридическая ответственность. Значение законности и правопорядка в современном обществе. Борьба с коррупцией. Основы частного права. Основы гражданского права. Понятие гражданского правоотношения. Физические и юридические лица. Основы семейного права. Брачно-семейные отношения. Основы трудового права. Трудовой договор. Трудовая дисциплина и ответственность за ее нарушение.  Основы публичного права. Административные правонарушения и административная ответственность. Правовые основы защиты государственной тайны. Законодательные и нормативно-правовые акты в области защиты информации и государственной тайны. Основы уголовного права. Понятие преступления. Экологическое право. Особенности правового регулирования будущей профессиональной деятельности.</p>	
<p><b>Б1.Б.6</b></p>	<p><b>КУЛЬТУРОЛОГИЯ И МЕЖКУЛЬТУРНОЕ ВЗАИМОДЕЙСТВИЕ</b></p> <p><b>Цели изучения дисциплины:</b>  Целями освоения дисциплины являются:</p> <ul style="list-style-type: none"> <li>– формирование, закрепление и расширение базовых знаний о культурологии как науке и о культуре как предмете культурологии; об основных разделах современного культурологического знания и о проблемах и методах их исследования;</li> <li>– 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.</li> </ul> <p><b>Задачи дисциплины:</b></p> <ul style="list-style-type: none"> <li>– раскрыть сущность культуры;</li> <li>– осмыслить уникальный исторический опыт диалога культур и способы его миропонимания;</li> <li>– представить современность как результат культурно-исторического развития человечества.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b>  Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения истории, русского языка и культуры речи.  Знания (умения, владения), полученные при изучении данной дисциплины, будут необходимы для изучения дисциплин «Иностранный язык в профессиональной деятельности», «Медиакультура».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОК-6</b> способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия  <b>ОК-7</b> способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности</p>	



	<p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук;</li> <li>- основные этапы развития философской мысли, основную проблематику и структуру философского знания;</li> <li>- школы и концепции культурологии, формы культуры, основы истории мировой и отечественной культуры.</li> </ul> <p>материальную и духовную роль культуры в развитии современного общества;</p> <ul style="list-style-type: none"> <li>- закономерности культурных процессов, функции культурных институтов и значение культурных норм в жизнедеятельности общества;</li> </ul> <p>развития и роль отечественной культуры в развитии современной цивилизации.</p> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>-использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач;</li> <li>- анализировать мировоззренческие, социально и личностно значимые философские проблемы;</li> <li>- использовать культурные нормы, регулирующие отношение человека к человеку, обществу, окружающей среде, использовать данные знания при разработке социальных проектов и в различных сферах жизнедеятельности.</li> <li>-оценивать альтернативы общественного развития с учетом культурных реалий.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- публичной речи, аргументации, ведения дискуссии и полемики;</li> <li>-анализа и оценки культурных процессов и явлений, планировать и осуществлять свою деятельность с учетом результатов этого анализа;</li> <li>- восприятия и анализа социальных и профессиональных проблем на основе нравственных ценностей, социальных принципов гражданской позиции, патриотизма, гуманизма.</li> <li>- культурного взаимодействия в поликультурной и полиэтничной среде на основе принятых в обществе моральных и правовых норм</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Культурология в системе научного знания. Становление культурологии как науки. Основные теории происхождения культуры. История культурологических учений и типология культуры. Представления о культуре от Античности до XVII века. Концепции культуры XVIII – XIX вв.. Основные направления в современной культурологии. Дихотомия восточного и западного типа культур. Основные понятия культурологии. Культура, её ценности и нормы, культурная картина мира. Основные формы и типы культуры. Культура как система знаков.</p>	
<p><b>Б1.Б.7</b></p>	<p><b>ТЕХНОЛОГИЯ КОМАНДООБРАЗОВАНИЯ И САМОРАЗВИТИЯ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>формирование у студентов универсальных, общепрофессиональных и профессиональных компетенций, позволяющих им успешно решать весь спектр задач, связанных с созданием и функционированием команд в организациях, а также отчетливо выраженного индивидуального взгляда на проблему создания и функционирования управленческой команды, понимания ее сути как социально-психологического феномена.</p> <p><b>Задачи изучения дисциплины:</b></p> <ul style="list-style-type: none"> <li>- сформировать у студентов научно обоснованное представление о команде, как фундаментальном понятии современной организационной психологии, и о социально-психологической сущности его</li> </ul>	

феноменологического содержания в организационном контексте;

- обучить студентов практическим методам отбора кандидатов в различного типа команды в логике обеспечения кадрового потенциала, интеграции функций оперативного управления, и перспективного развития организации;
- обучить студентов самостоятельной разработке и реализации развернутых программ социально-психологического обеспечения, создания команд с учетом специфики конкретных организаций;
- обеспечить личностное и профессиональное развитие студентов применительно к реализации функции командного оператора;
- сформировать у студентов целенаправленную установку на ознакомление с практическим опытом коллег, систематический анализ как окончательных, так и промежуточных результатов деятельности, в контексте командообразования;
- расширить компетенции студентов, связанные с практической социально-психологической работой, по интрагрупповому развитию в широком контексте;
- обучить студентов методологическим и методическим основам систематизации собственного практического опыта и разработки на его основе авторских командообразующих техник и технологий.

**Место дисциплины в структуре ООП:**

Дисциплина «Технология командообразования и саморазвития» входит в базовую часть блока Б1

Изучение дисциплины «Технология командообразования и саморазвития» базируется на знаниях дисциплин «Культурология и межкультурное взаимодействие» и «Медиакультура»

При изучении дисциплины создаются основы для освоения процесса взаимодействия с коллективом во время прохождения учебной и производственной практики, а также основ саморазвития и командной работы в процессе научно-исследовательской работы.

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ОК – 6:** способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность

**В результате изучения дисциплины студент должен:**

**знать:**

основные понятия по командообразованию, основы психологической безопасности взаимодействия в команде, способы действий в нестандартных и конфликтных ситуациях, которые происходят в команде; технологии организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности

**уметь:**

определять угрозы психологической безопасности и способы ее предотвращения в процессе взаимодействия; этично относиться к другим членам команды; нести ответственность за принятые решения; формулировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения; осуществления деятельности.

**владеть навыками:**

бесконфликтного общения; этичного взаимодействия в команде в процессе решения профессиональных задач; технологиями организации процесса самообразования; приемами целеполагания во временной перспективе,

	<p>способами планирования, организации, самоконтроля и самооценки деятельности.</p> <p><b>Дисциплина включает в себя следующие разделы:</b>          Команда как вид групп высшего уровня развития. Формирование команды. Распределение ролей и особенности работы в команде. Управление взаимоотношениями в команде. Коммуникации в команде. Управление конфликтами в командах. Жизненный путь личности и саморазвитие. Индивидуальный коучинг.</p>	
<p><b>Б1.Б.8</b></p>	<p align="center"><b>БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ</b></p> <p><b>Цели изучения дисциплины:</b>          Целями освоения дисциплины «Безопасность жизнедеятельности» является формирование знаний и навыков, необходимых для создания безопасных условий деятельности при проектировании и использовании техники и технологических процессов, а также при прогнозировании и ликвидации последствий стихийных бедствий, аварий и катастроф.</p> <p><b>Место дисциплины в структуре ООП:</b>          Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения «Истории Отечества», «Культурологии», «Физики», «Информатики».          Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы при изучении дисциплин «Разработка и эксплуатация защищенных автоматизированных систем», «Анализ рисков информационной безопасности».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОК-7</b> способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- опасные и вредные факторы системы "человек - среда обитания";</li> <li>- научные и организационные основы защиты среды и ликвидации;</li> <li>- последствий аварий, катастроф, стихийных бедствий;</li> <li>- основные нормы и правила техники безопасности;</li> <li>- основные опасные и вредные производственные факторы</li> <li>- основные техносферные опасности, их свойства и характеристики;</li> <li>- основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности;</li> <li>- применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;</li> <li>- готовить устные (письменные) сообщения по методам исследований БЖД;</li> <li>- выбирать эффективные методы защиты;</li> <li>- самостоятельно находить информацию о совершенствовании методов защиты от основных техносферных опасностей.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками безопасного использования технических средств в профессиональной деятельности;</li> <li>- приемами основных методов исследований БЖД;</li> <li>- навыками использования понятийно-терминологического аппарата в области безопасности</li> <li>- навыками измерения уровня ОВПФ в производственных условиях.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p>	<p>108 (3)</p>

	<p>Теоретические основы дисциплины. Основы физиологии труда. Правовые и организационные основы безопасности жизнедеятельности. Производственная санитария. Условия труда на производстве. Методы и средства обеспечения безопасности производственного оборудования и технологических процессов. Основные понятия о чрезвычайных ситуациях. Защита населения и территории от чрезвычайных ситуаций природного и техногенного характера. Правовые и организационные вопросы охраны окружающей среды. Технические и технологические решения задач охраны окружающей среды. Безопасность и экологичность производств. Экономическая оценка опасной деятельности.</p>	
<p><b>Б1.Б.9</b></p>	<p style="text-align: center;"><b>ФИЗИКА</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины являются:</p> <ul style="list-style-type: none"> <li>- ознакомление с фундаментальными понятиями, законами и теориями классической и современной физики;</li> <li>- приобретение навыков экспериментального исследования физических процессов, освоение методов получения и обработки эмпирической информации;</li> <li>- изучение теоретических методов описания физических явлений, применяемых в современной физике.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b> полученных в общеобразовательной школе: дифференциальное и интегральное исчисление, начала векторного анализа. Из школьного курса химии необходимо знание следующих разделов: периодическая система элементов и ее структура, строение атома, основные законы химии, электрохимия.</p> <p>ФИЗИКА является необходимой в изучении последующих дисциплин: « Основы радиотехники», «Электроника и схемотехника», «Техническая защита информации», «Физические основы передачи информации».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-7</b> 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 систем с учетом нормативных требований по защите информации. <b>ПК-18</b> способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b> <b>знать:</b> основные законы механики; - основные законы термодинамики и молекулярной физики; - основные законы электричества и магнетизма; - основы теории колебаний и волн, оптики; - основы квантовой физики и физики твердого тела; - физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем; - методы физического моделирования материалов и технологических процессов.</p> <p><b>уметь:</b> - строить математические модели физических явлений и процессов; - решать типовые прикладные физические задачи; - анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;</p>	<p>540 (15)</p>

	<p>применять математические методы, физические и химические законы для решения практических задач,</p> <ul style="list-style-type: none"> <li>- проводить измерения, обрабатывать и представлять результаты.</li> <li>- применять физические законы для решения практических задач;</li> <li>- оценивать случайные ошибки эксперимента, определять доверительный интервал;</li> <li>- выбирать приборы с пределами измерений, необходимыми для данных измерений, определять цену деления, показания приборов, погрешность и уметь градуировать шкалу приборов;</li> <li>- составлять отчеты по выполненным экспериментальным работам, уметь делать выводы;</li> <li>- обоснованно выбирать и применять методику проведения эксперимента, профессионально эксплуатировать современное оборудование и приборы.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- методами теоретического исследования физических явлений и процессов;</li> <li>- навыками проведения физического эксперимента и обработки его результатов</li> <li>- навыками практического применения законов физики,</li> <li>- методами математического описания физических процессов и явлений, определяющих принципы работы различных технических устройств;</li> <li>- навыками проведения, анализа, теоретического и экспериментального исследования работоспособности и эффективности применяемой аппаратуры.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Классическая и релятивистская механика. Молекулярная физика и термодинамика. Электромагнетизм. Волновая оптика. Квантовая физика. Физика атома и ядра.</p>	
<p><b>Б1.Б.10</b></p>	<p style="text-align: center;"><b>ОСНОВЫ УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ</b></p> <p><b>Цели изучения дисциплины:</b>  Целями освоения являются:</p> <ul style="list-style-type: none"> <li>- понимание природы и сущности управления социально-экономическими системами;</li> <li>- знание законов и закономерностей управления,</li> <li>- знание принципов управления, формы и методы управления.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b>  Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения культурология, основы теории оптимизации.  Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы при изучении таких дисциплин, как: управление информационной безопасностью, информационная безопасность систем организационного управления.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОК-7</b> 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  <b>ПК-18</b> способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b>  <b>знать:</b></p> <ul style="list-style-type: none"> <li>- научные основы, цели, принципы, методы и технологии управленческой деятельности;</li> <li>способы формирования целей команды;</li> </ul>	<p><b>72 (2)</b></p>

	<p>- порядок принятия организационно-управленческие решений в нестандартных ситуациях и нести за них ответственность;</p> <p>- научные основы цели, принципы, методы воспитательной и образовательной деятельности;</p> <p>- методы предупреждения конфликтных ситуаций в процессе профессиональной деятельности.</p> <p><b>уметь:</b></p> <p>- работать в коллективе, принимать управленческие решения и оценивать их эффективность;</p> <p>- вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности.</p> <p><b>владеть навыками:</b></p> <p>- навыками выбора, обоснования, реализации и контроля результатов управленческого решения;</p> <p>- практическими навыками работы в коллективе в качестве руководителя;</p> <p>- способностью разрабатывать оперативные планы работы первичных подразделений.</p> <p><b>Дисциплина включает в себя следующие разделы:</b>  Основные положения теории социального управления. Сущность и виды социального управления. Цели и задачи управленческой деятельности. Организационная структура системы управления. Место и роли руководителя в системе управления. Специфика должностного положения руководителя. Формирование руководящего ядра. Особенности правового регулирования труда руководителя.</p>	
<p><b>Б1.Б.11</b></p>	<p style="text-align: center;"><b>АЛГЕБРА И ГЕОМЕТРИЯ</b></p> <p><b>Цели изучения дисциплины:</b>  Целью дисциплины является обеспечение фундаментальной подготовки в одной из важнейших областей современной математики; формирование навыков решения геометрических задач в различных системах координат; ознакомление с основами классической и современной алгебры; обучение основным алгебраическим методам решения задач, возникающих в других математических дисциплинах и в практике; ознакомление с историей развития алгебры и геометрии, с вкладом российских ученых в развитие современной алгебраической науки.</p> <p>Задачами дисциплины являются:</p> <ul style="list-style-type: none"> <li>– начальная общематематическая подготовка студентов путем изучения достаточно простых математических конструкций, которые в последующих математических дисциплинах будут обобщаться,</li> <li>– обучение простейшей алгебраической структуре - векторной алгебре и ее приложениям, формирование навыков использования координатного метода,</li> <li>– формирование навыков применения алгебраических методов для упрощения уравнений линий и поверхностей второго порядка,</li> <li>– ознакомление с различными алгебраическими структурами (кольцами, полями, векторными пространствами) и их приложениями в решении различных практических задач,</li> <li>– освоение методов линейной алгебры широко используемых в различных дисциплинах, в том числе профессиональных,</li> <li>– воспитание у студентов математической и технической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для специалиста в области информационной безопасности.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b>  Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:</p> <ul style="list-style-type: none"> <li>– Знания, умения и навыки сформированные в процессе изучения</li> </ul>	<p><b>180 (5)</b></p>

программы общеобразовательной школы.

Знания, полученные при изучении дисциплины «Алгебра и геометрия», используются при изучении следующих дисциплин: Математический анализ, Дискретная математика, Математическая логика и теория алгоритмов, Теория вероятностей и математическая статистика, Теория информации, Технологии и методы программирования, Криптографические методы защиты информации, Физика, Криптографические методы защиты информации

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**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 алв работе над междисциплинарными и инновационными проектами.

**В результате изучения дисциплины студент должен:**

**знать:**

- основные понятия и задачи векторной алгебры и аналитической геометрии;
- основные свойства алгебраических структур;
- основы линейной алгебры над произвольными полями;
- основные возможности координатного метода для исследования различных геометрических объектов, задачи векторной алгебры и аналитической геометрии, виды уравнений простейших геометрических объектов, свойства важнейших алгебраических структур.

**уметь:**

- решать основные задачи векторной алгебры и аналитической геометрии;
- строить и изучать основные математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, определять основные возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач, исследовать простейшие геометрические объекты по их уравнениям в различных системах координат, оперировать с числовыми и конечными полями, многочленами, матрицами, решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями.

**владеть навыками:**

- навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;
- методами линейной алгебры;
- навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры.

**Дисциплина включает в себя следующие разделы:**

Предмет курса. Принципы построения и изучения курса. Краткое содержание. Некоторые сведения из теории определителей и систем линейных уравнений. Определители матриц второго и третьего порядка. Системы линейных уравнений. Элементарные преобразования систем. Равносильные системы. Векторная алгебра. Линейные операции с векторами плоскости (пространства) и их свойства. Базисы плоскости и пространства. Координаты векторов в базисе. Скалярное, векторное, смешанное и двойное векторное произведение векторов. Свойства рассматриваемых операций над векторами. Системы координат и простейшие задачи, решаемые с использованием векторной алгебры. Прямая линия на плоскости. Эллипс, гипербола, парабола. Вывод их уравнений и описание простейших свойств. Оптические свойства эллипса, гиперболы и параболы. Прямая и плоскость в пространстве. Различные уравнения плоскости. Поверхности второго порядка. Основные алгебраические структуры. Бинарные операции на множестве и их

	<p>классификация. Группоиды, полугруппы. Нейтральные и симметричные элементы. Полугруппа преобразований. Матрицы над кольцами. Определители матриц. Обратимые матрицы. Матрицы над полями и системы линейных уравнений. Линейная зависимость векторов арифметических пространств. Подпространства арифметических пространств. Числовые кольца и поля. Кольца вычетов. Кольца многочленов. Линейные пространства. Подобие матриц над полем. Линейные преобразования евклидовых пространств.</p>	
<p><b>Б1.Б.12</b></p>	<p style="text-align: center;"><b>МАТЕМАТИЧЕСКИЙ АНАЛИЗ</b></p> <p><b>Цели изучения дисциплины:</b>  Цель 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.  Задача дисциплины – привить обучаемым навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни.</p> <p><b>Место дисциплины в структуре ООП:</b>  Для успешного усвоения данной дисциплины необходимо, чтобы обучаемый владел знаниями, умениями и навыками, сформированными в процессе изучения математики в средней школе, а также дисциплины «Алгебра и геометрия».  Знания, полученные обучаемыми по дисциплине «Математический анализ», непосредственно используются при изучении дисциплин базового цикла: «Физика», «Теория вероятностей и математическая статистика», «Теория информации».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОК-2</b> способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов</p> <p><b>В результате изучения дисциплины студент должен:</b>  <b>знать:</b>  - основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;  - основные положения теории пределов и непрерывных функций, теории числовых и функциональных рядов,  - основные понятия теории функций комплексной переменной;  - основные методы решения простейших дифференциальных уравнений и систем дифференциальных уравнений</p> <p><b>уметь:</b>  - решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды;  - оперировать с числовыми многочленами, матрицами;  - решать основные задачи линейной алгебры, системы линейных уравнений над полями;  - строить и изучать математические модели конкретных явлений и процессов для решения расчётных и исследовательских задач;  - определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; решать основные задачи на вычисление пределов функций,</p>	<p><b>252 (7)</b></p>



	<p>дифференцирование и интегрирование, на разложение функций в ряды.</p> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач;</li> <li>- решения задач с применением аппарата теории функций комплексной переменной; навыками использования стандартных методов решения типовых дифференциальных уравнений;</li> <li>- пользования библиотеками прикладных программ для решения прикладных математических задач.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>          Действительные числа. Понятие функции. Теория пределов числовых последовательностей и числовых рядов. Теория пределов функций одной действительной переменной. Непрерывность функций одной действительной переменной. Дифференциальное исчисление функций одной действительной переменной. Приложения дифференциального исчисления функций одной действительной переменной. Теория пределов, непрерывность. Дифференцируемость функции многих действительных переменных. Неопределенный интеграл. Определенный интеграл. Кратные интегралы. Криволинейные и поверхностные интегралы. Комплексные числа и функции комплексной переменной. Дифференцирование и интегрирование функций комплексной переменной. Дифференциальные уравнения 1-го порядка. Линейные дифференциальные уравнения n-го порядка. Функциональные последовательности и ряды в действительной области. Функциональные ряды в комплексной области. Теория вычетов. Ряды Фурье. Преобразование и интеграл Фурье.</p>	
<p><b>Б1.Б.13</b></p>	<p style="text-align: center;"><b>Теория вероятностей и математическая статистика</b></p> <p><b>Цели изучения дисциплины:</b>          Целями 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 (инженерных задач) и овладение основными методами исследования и решения таких задач, выработка у студентов умения проводить статистический анализ прикладных (инженерных задач) и овладение основными методами исследования и решения таких задач.</p> <p><b>Задачами изучения дисциплины являются:</b></p> <ul style="list-style-type: none"> <li>- изучение природы случайных событий и способов их математического описания, построение алгебры событий вычисление вероятностей;</li> <li>- изучение случайных величин как функций на алгебре событий, их распределений и числовых характеристик;</li> <li>- изучение законов больших чисел и их применимости при исследовании массовых явлений.</li> <li>- развитие логического и алгоритмического мышления;</li> <li>- изучение методики обработки статистических данных, оценок параметров распределения, теории проверки статистических гипотез, корреляционного и регрессионного анализа;</li> <li>- овладение основными методами исследования и решения статистических задач;</li> <li>- выработку умения самостоятельно расширять статистические знания и проводить вероятностный анализ прикладных (инженерных) задач;</li> <li>- реализация основных алгоритмов исследования средствами программного обеспечения и вычислительной техники.</li> </ul>	<p><b>108 (3)</b></p>

**Место дисциплины в структуре ООП:**

Изучение дисциплины базируется на следующих курсах: алгебра и геометрия, математический анализ, дискретная математика, теория и практика обработки информации, программирование. Изучающий дисциплину студент должен владеть аппаратом математического анализа, иметь навыки комбинаторных рассуждений, уметь пользоваться аксиомами и теоремами булевой алгебры, уметь пользоваться пакетами прикладных программ для практических расчетов, уметь решать вероятностные задачи и пользоваться пакетами прикладных программ для обработки результатов наблюдений

Дисциплина является предшествующей для изучения дисциплин: математическое моделирование, защита информации, нейрокомпьютерные системы, основы теории управления, обработка экспериментальных данных на ЭВМ.

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**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 алгебры.

**В результате изучения дисциплины студент должен:****знать:**

- природу случайных событий и способов их математического описания, построение алгебры событий вычисление вероятностей;
- законы больших чисел и их применимости при исследовании массовых явлений.
- методику обработки статистических данных, оценок параметров распределения, теории проверки статистических гипотез, корреляционного и регрессионного анализа;

**уметь:**

- самостоятельно расширять статистические знания и проводить вероятностный анализ прикладных (инженерных) задач;

**владеть навыками:**

- основными методами исследования и решения статистических задач;
- реализации основных алгоритмов исследования средствами программного обеспечения и вычислительной техники.

**Дисциплина включает в себя следующие разделы:**

Классическое, геометрическое и статистическое определение вероятности. Теоремы сложения и умножения. Условная вероятность. Формула полной вероятности и формула Байеса. Схема Бернулли, приближения Лапласа и Пуассона.

Дискретные и непрерывные случайные величины. Ряд распределения, функция распределения и плотность. Математическое ожидание и дисперсия. Неравенство и теорема Чебышёва. Нормальное и другие распределения. Центральная предельная теорема.

Генеральная совокупность и выборка. Статистическое распределение, эмпирическая функция распределения. Полигон и гистограмма. Статистические точечные оценки параметров распределения. Методы получения статистических оценок. Интервальные оценки параметров распределения. Доверительные интервалы для параметров нормального распределения.

Статистическая гипотеза и общая схема ее проверки. Ошибки 1 и 2 рода. Уровень значимости и мощность критерия. Критерии значимости и критерии согласия Критерий согласия Пирсона для проверки гипотезы о нормальном распределении. Функциональная, статистическая и корреляционная зависимости. Линейная парная корреляция, коэффициент корреляции. Корреляционное отношение и индекс корреляции. Многомерный корреляционный анализ.

<p><b>Б1.Б.14</b></p>	<p style="text-align: center;"><b>ДИСКРЕТНАЯ МАТЕМАТИКА</b></p> <p><b>Цели изучения дисциплины:</b>  Целями освоения дисциплины «Дискретная математика» являются: ознакомление студентов с основными понятиями дискретной математики, формирование у студентов понимания теоретических основ современной теории алгоритмов, теории компиляции, теории верификации программ, выработка соответствующего категориального аппарата.  Для достижения поставленных целей в курсе «Дискретная математика» решаются задачи:</p> <ul style="list-style-type: none"> <li>К освоение математического аппарата, являющегося теоретической основой современного программирования и его практических приложений;</li> <li>К изучение основных идей комбинаторики;</li> <li>К освоение понятий алгебры логики и приобретение навыков работы с ними;</li> <li>К изучение теоретических основ теории графов и ее применения.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b>  Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения алгебры и геометрии, математического анализа.  Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: исследование операций и теория игр, теория графов и её приложения, базы данных, математическое моделирование распределенных систем, основы информационной безопасности, сети и системы передачи информации и др.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОПК-2</b> способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основные понятия и методы, алгебр высказываний и логики, теории множеств и комбинаторики, теории графов, теории автоматов и принципы использования понятий и методов дискретной математики в смежных областях с несущественными ошибками;</li> <li>- основные понятия теории автоматов;</li> <li>- основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры;</li> <li>- методы перечисления для основных дискретных структур;</li> <li>- общие формы, закономерности и инструментальные средства дискретной математики и математической логики.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач;</li> <li>- самостоятельно сформулировать задачу исследований дискретного объекта, используя теоретико-множественные, логические и графические средства конструктивного анализа и моделирования;</li> <li>- переходить от одной формы математического представления дискретной модели к другой.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками построения дискретных моделей при решении профессиональных задач;</li> </ul>	<p>144 (4)</p>

	<p>основными понятиями и методами математической логики, навыками моделирования прикладных задач методами дискретной математики, а также навыками их использования в смежных областях;</p> <p>самостоятельными навыками построения и анализа математических моделей типичных задач.</p> <p><b>Дисциплина включает в себя следующие разделы:</b>  Метод математической индукции и комбинаторика. Элементы теории множеств. Множества и их спецификации. Отношения. Операции над множествами. Элементы теории графов. Способы задания графов. Лес и деревья. Переключательные функции. Основные функции одной и двух переменных. Аналитическое представление переключательных функций. Минимизация переключательных функций и контактные схемы. Алгебра Жегалкина. Примеры замкнутых классов. Примеры функционально полных систем и базисов.</p>	
<p><b>Б1.Б.15</b></p>	<p align="center"><b>МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ</b></p> <p><b>Цели изучения дисциплины:</b>  Целью дисциплины является усвоение студентами базовых понятий теории математической логики и теории алгоритмов, использование их для решения прикладных задач, а также формирование общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по специальности 090303 Информационная безопасность автоматизированных систем.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– усвоение основных положений теории математической логики;</li> <li>– повышение уровня логической подготовки студентов, предполагающего умение проводить согласующиеся с логикой математические рассуждения;</li> <li>– применение при проектировании вычислительной техники и автоматизированных систем.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b>  Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин: «Алгебра и геометрия», «Математический анализ», «Информатика», «Языки программирования». Знания (умения, навыки), полученные при изучении дисциплины «Математическая логика и теория алгоритмов», будут необходимы при дальнейшем изучении таких дисциплин, как «Исследование операций и теория игр», «Теория графов и ее приложения».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОПК-2</b> способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики;</li> <li>- основы комбинаторного анализа;</li> <li>- основные понятия математической логики и теории алгоритмов;</li> <li>-- формальный язык логики и логики предикатов;</li> <li>- формализации понятия алгоритма: машины Тьюринга, рекурсивные функции;</li> <li>- основные понятия теории сложности алгоритмов;</li> </ul>	<p>180 (5)</p>

	<ul style="list-style-type: none"> <li>- алгоритмы приведения булевых функций к нормальной форме и построения минимальных форм;</li> <li>- специальные классы булевых функций методы исследования системы булевых функций на полноту,</li> <li>- основные принципы логического программирования, элементы алгоритмической логики;</li> <li>- понятия формализации понятия алгоритма: машины Тьюринга, рекурсивные функции, алгоритмы Маркова;</li> <li>- основные понятия теории сложности алгоритмов.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;</li> <li>- строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;</li> <li>-исследовать булевы функции, получать их представление в виде формул;</li> <li>- производить построение минимальных форм булевых функций;</li> <li>- определять полноту и базис системы булевых функций;</li> <li>- выбирать и применять математические методы, физические законы и вычислительную технику для формализации, анализа и выработки решения практических задач;</li> <li>- оценивать сложность алгоритмов и вычислений.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач;</li> <li>- основными методами исследования булевых функций;</li> <li>- применения булевых функций для построения релейно-контактных схем;</li> <li>- использования булевых функций для решения исследовательских задач;</li> <li>- применения физико-математического аппарата для решения прикладных задач;</li> <li>- по выявлению алгоритмически неразрешимых, легко и трудно разрешимых проблем;</li> <li>- применения алгебры высказываний и логики предикатов для решения прикладных теоретико-информационных задач.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>          Логика высказываний. Высказывания и операции над ними. Формулы алгебры высказываний. Булевы функции. Множества, отношения, функции. Формализованное исчисление высказываний. Система аксиом и теория формального вывода. Логика предикатов. Основные понятия, связанные с предикатами. Равносильность и следование предикатов. Формулы логики предикатов. Элементы теории алгоритмов. Машины Тьюринга. Рекурсивные функции. Нормальные алгоритмы Маркова. Алгоритмы и разрешимость. Логическое программирование. Основные конструкции языка программирования Пролог. Рекурсивное программирование. Метод отсечения и отката. Метод повтора. Списки и их использование. Вычислительная модель логических программ.</p>	
<p><b>Б1.Б.16</b></p>	<p style="text-align: center;"><b>ТЕОРИЯ ИНФОРМАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b>          Целями освоения дисциплины «Теория информации» является формирование у студентов понятий об основных принципах теории информации; информации, о подходах к измерению информации, о кодировании, о алгоритмах перекодирования (эффективное кодирование). Подробно рассматривается: теория информации Шенона; алгоритмы Шенона–Фано, Хаффмана, Лемпеля-Зива; понятие и применение блочного помехозащищенного кода; совершенные и квазисовершенные</p>	<p><b>180(5)</b></p>

	<p>помехозащищенные коды; современные алгоритмы шифров шифрования с симметричным и несимметричным ключом. Овладение студентами необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Для усвоения данной дисциплины студенту необходим объем знаний, предусмотренный курсами информатики, организации ЭВМ и вычислительных систем и высшей математики (теория вероятности, математический анализ, векторная алгебра, элементарные знание дискретной математики, систем исчисления).</p> <p>Данная дисциплина необходима для последующего успешного освоения следующих дисциплин: «Физические основы защиты информации», «Сети и системы передачи информации», «Техническая защита информации», «Безопасность сетей ЭВМ».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ОПК-2.</b> Способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b> Физический смысл условной, взаимной и полной энтропии системы передачи информации Вероятностные характеристики источника сообщений, канала связи и приемника сообщений</p> <p><b>уметь:</b> Уметь выполнять преобразования информации повышающие и понижающие ее избыточность Определять основные характеристики канала связи по информации о передаваемых величина</p> <p><b>владеть навыками:</b> Способностью выполнять прямое и обратное преобразование информации по алгоритму Лемпеля-Зива и Хемминга Способностью выполнять прямое и обратное преобразование информации по арифметическому алгоритму, по динамическому алгоритму Хаффмана, динамическому арифметическому алгоритму</p> <p><b>Дисциплина включает в себя следующие разделы:</b> Основы теории информации. Методы кодирования основанные на статистических параметрах. Помехоустойчивые коды.</p>	
<p><b>Б1.Б.17</b></p>	<p style="text-align: center;"><b>ИНФОРМАТИКА</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Информатика» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем. Задачи дисциплины: формирование представлений об основных принципах информатики, сферах ее применения, перспективах развития, способах функционирования и использования информационных технологий решения задач. Приоритетными объектами изучения информатики являются информационные системы, связанные с информационными процессами, и информационные технологии, рассматриваемые с позиций системного подхода.</p>	<p>432 (12)</p>

**Место дисциплины в структуре ООП:**

Дисциплина «Информатика» входит в цикл дисциплин Б1.Б.17 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Для освоения дисциплины студенты используют знания, умения и компетенции, сформированные в ходе изучения базового курса «Информатика» в объеме средней общеобразовательной школы.

Дисциплина является предшествующей для изучения дисциплин: «Языки программирования», «Информационные технологии. Базы данных», «Теория информации», «Сети и системы передачи информации», «Технологии и методы программирования», «Основы информационной безопасности», «Основы теории оптимизации».

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ОПК-4** - способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах;

**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.

**В результате изучения дисциплины студент должен:****знать:**

- Значение информации в развитии современного общества;
- Современные способы использования компьютерных технологий для проведения исследований.

**уметь:**

- Эффективно использовать современные компьютерные технологии для изучения предмета исследования;
- Эффективно использовать и оптимизировать свою работу для обмена данными, с использованием глобальной информационной сети Интернет и библиотечными фондами.

**владеть:**

- Способами повышения эффективности использования информационных технологий для решения профессиональных задач;
- Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.

**Дисциплина включает в себя следующие разделы:**

Основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды. Формы и способы представления данных в персональном компьютере. Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера. Типовые структуры и принципы организации компьютерных сетей. Обеспечение безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией). Работа с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов). Использование языков, систем и инструментальных средств программирования в профессиональной

	<p>деятельности. Алгоритмизация и программирование. Языки программирования высокого уровня. 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. Использование библиотек прикладных программ для решения прикладных математических задач.</p>	
<p><b>Б1.Б.18</b></p>	<p style="text-align: center;"><b>ИССЛЕДОВАНИЕ ОПЕРАЦИЙ. ТЕОРИЯ ИГР</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью освоения дисциплины «Исследование операций и теория игр» является обучение студентов основам теории игр и исследования операций.</p> <p>Задачами изучения дисциплины являются:</p> <ul style="list-style-type: none"> <li>• ознакомить студентов с основными математическими методами для обоснования решений в различных областях целенаправленной человеческой деятельности;</li> <li>• формировать у студентов умение формализовать реальную ситуацию, создавать правильную математическую модель, грамотно использовать математические методы.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Математический анализ, Теория вероятностей и математическая статистика.</p> <p>Последующими дисциплинами являются: Методы оптимизации, Моделирование автоматизированных информационных систем.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПСК-7.1-</b>Способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>-основные понятия, идеи и приемы исследования операций и теории игр, необходимые для применения в своей предметной области и в повседневной практике;</li> <li>-методы и алгоритмы разработки моделей исследования операций и теории игр без ошибок с привлечением дополнительной литературы и Интернет-ресурсов.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- применять методы исследования операций и теории игр при разработке и исследования моделей информационно-технологических ресурсов;</li> <li>- разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками самостоятельного применения методов исследования операций и теории игр при разработке и исследования моделей информационно-технологических ресурсов;</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Введение в исследование операций. Основные понятия и методологические основы исследования операций.</p> <p>Одномерный поиск (метод прямого поиска, метод половинного деления, метод дихотомии, метод золотого сечения).</p> <p>Методы динамического программирования в исследовании операций. Задача о замене оборудования.</p> <p>Методы линейного программирования в исследовании операций. Задача о назначениях. Графический метод решения задач линейного программирования. Симплекс-метод.</p>	<p><b>144 (4)</b></p>



	<p>Введение в теорию массового обслуживания. Задачи массового обслуживания в рамках исследования операций.</p> <p>Введение в теорию игр. Матричные игры. Решение матричных игр в чистых стратегиях. Принцип минимакса и максимина. Доминирующие стратегии.</p> <p>Игры с природой. Принятие решений в условиях неопределенности. Принятие решений в условиях риска.</p>	
<p><b>Б1.Б.19</b></p>	<p style="text-align: center;"><b>ТЕОРИЯ ГРАФОВ И ЕЕ ПРИЛОЖЕНИЯ</b></p> <p><b>Цель дисциплины:</b> Целями освоения дисциплины являются: знакомство с фундаментальными понятиями и математическим аппаратом теории графов; изучение основных задач теории графов и методов их решения, формирование навыков эффективно применять графовые модели для решения прикладных задач, использовать компьютер для реализации графовых алгоритмов.</p> <p><b>Место дисциплины в структуре ООП:</b> Дисциплина «Теория графов и ее приложения» входит в математический и естественно научный цикл образовательной программы по специальности 090303 Информационная безопасность автоматизированных систем.</p> <p>Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Математический анализ», «Дискретная математика», «Информатика», «Языки программирования», «Математическая логика и теория алгоритмов», «Технологии и методы программирования».</p> <p>Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Математическое моделирование распределенных систем», «Информационная безопасность распределенных информационных систем», «Моделирование систем и процессов защиты информации», «Информационная безопасность систем организационного управления».</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения «Теория графов и ее приложения» направлен на формирование следующих компетенций:</p> <p><b>ПК-4</b> способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p><b>ПСК 7.1</b> способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студенты должны:</b></p> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>К общую постановку задач теории графов;</li> <li>К основные принципы построения графов с заданными свойствами</li> <li>К связи теории графов с другими предметами, различные информационные технологии, используемые в теории графов</li> <li>К Новые технологии применения теории графов в теории игр, социологии, проектировании сетей и других прикладных задачах</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>К Применять методы теории графов при решении задач на ЭВМ</li> <li>К Самостоятельно приобретать знания и применять теорию графов при решении задач на ЭВМ</li> <li>К Приобретать новые знания и методы использования графов при программировании</li> <li>К Классифицировать задачи теории графов по степени сложности и применять соответствующие алгоритмы для решения задач</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>К Методологическими основами формирования изучения графов и их свойств при исследовании и построении систем</li> <li>К Приемами исследования проблем области теории графов, возникающих в различных сферах человеческой деятельности</li> <li>К Навыками решения оптимизационных задач теории графов и задач сетевого планирования</li> </ul>	<p><b>108 (3)</b></p>

	<p>К Навыками проектирования информационных структур  К Навыками применения математического аппарата для решения прикладных теоретико-информационных задач</p> <p><b>Основные (разделы):</b> Введение в теорию графов. Способы машинного представления графов. Виды графов, подграфы, операции над графами. Обходы графов. Маршруты, цепи, пути, циклы. Связность, компоненты связности. Обходы графов: виды обходов, реализация обходов. Разрезания и раскраска графов. Понятие разреза. Задача о разрезании графа. Разрезание различных видов графов. Понятие раскраски, хроматического числа. Задача о вершинной раскраске, о раскраске граней, их связь. Оценка хроматического числа для некоторых видов графов. Оптимизационные задачи на графах. Поиск кратчайших путей. Алгоритмы Форда-Беллмана, Флойда, Дейкстры, поиск пути в бесконтурном графе. Задача о потоке. Задача о каркасе минимального веса. Задача коммивояжера. Сетевое планирование. Прикладные задачи теории графов. Применение рассмотренных алгоритмов для решения прикладных задач. Применение графов для задач программирования, графы как модели программ, процессов, информационных структур.</p> <p><b>Общая трудоемкость дисциплины</b> Общая трудоемкость дисциплины составляет <b>3 зачетных единицы 108 часов:</b> аудиторные часы – 54 часа, самостоятельная работа – 54 часа, курсовая работа. Основные виды учебной работы: лекции; практические занятия; СРС. Форма проведения аттестации – зачет и курсовая работа.</p>	
<p><b>Б1.Б.20</b></p>	<p style="text-align: center;"><b>ЯЗЫКИ ПРОГРАММИРОВАНИЯ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Языки программирования» является изучение языков программирования высокого уровня и формирования у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Языки программирования» рассматривает основные подходы к проектированию программных средств, освоению методологий структурного и объектно-ориентированного программирования, а также методов тестирования и отладки программ.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Языки программирования» входит в цикл дисциплин Б1.Б.20 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p>Успешное усвоение материала предполагает знание студентами основных положений курсов «Информатика» и «Организация ЭВМ и вычислительных систем».</p> <p>Дисциплина является предшествующей для изучения дисциплин: «Технологии и методы программирования», «Основы информационной безопасности», «Управление информационной безопасностью» «Моделирование угроз информационной безопасности», «Моделирование систем и процессов защиты информации», «Криптографические методы защиты информации» и др.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-10</b> - 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</p>	<p><b>324 (9)</b></p>

	<p>профессиональной деятельности.</p> <p><b>ОПК-3</b> - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- Язык программирования высокого уровня (объектно-ориентированное программирование).</li> <li>- Требования, предъявляемые к разработке внешних спецификаций, для разрабатываемого программного обеспечения.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- Формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения.</li> <li>- Проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения.</li> <li>- Проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- Навыками проектирования программного обеспечения с использованием средств автоматизации.</li> <li>- Навыками разработки сложного программного обеспечения.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Методики разработки программ. Языки программирования. Основы языка программирования Delphi. Организация взаимодействия приложения с пользователем. Технологии работы в Delphi. Создание пользовательских приложений.</p>	
<p><b>Б1.Б.21</b></p>	<p align="center"><b>ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ</b></p> <p><b>Цели освоения дисциплины</b></p> <p>Целью дисциплины является изучение основ современных методов и средств программирования и формировании у студентов 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.</p> <p><b>Место дисциплины в структуре ООП подготовки специалиста</b></p> <p>Успешное усвоение материала предполагает знание студентами основных положений курсов «Информатика», «Языки программирования» и «Организация ЭВМ и вычислительных систем».</p> <p>Дисциплина является предшествующей для изучения дисциплин: «Основы информационной безопасности», «Управление информационной безопасностью» «Моделирование угроз информационной безопасности», «Моделирование систем и процессов защиты информации» и др.</p> <p><b>Требования к результатам освоения дисциплины:</b></p> <p>Процесс изучения «Технологии и методы программирования» направлен на формирование следующих компетенций:</p> <p><b>ОПК-3</b> способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p><b>ПК-10</b> способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных</p>	<p><b>216 (6)</b></p>

	<p>компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>В результате изучения дисциплины студенты должны:</b></p> <p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>К язык программирования высокого уровня (объектно-ориентированное программирование); современные технологии и методы программирования; показатели качества программного обеспечения;</li> <li>К методологии и методы проектирования программного обеспечения; методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;</li> <li>К методы тестирования и отладки программного обеспечения способы; обработки исключительных ситуаций; принципы организации документирования разработки, процесса сопровождения программного обеспечения;</li> <li>К показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; профессиональных задач; методы тестирования и отладки программного обеспечения способы.</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>К проводить комплексное тестирование и отладку программных систем;</li> <li>К проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения; проводить выбор эффективных способов реализации профессиональных задач; планировать разработку сложного программного обеспечения;</li> <li>К формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; пользоваться нормативными документами по противодействию технической разведке;</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>К навыками программирования с использованием эффективных реализаций структур данных и алгоритмов;</li> <li>К навыками разработки программной документации; навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;</li> </ul> <p><b>Основные (разделы):</b></p> <p>Введение в технологии программирования. Проектирование и разработка архитектуры. Платформа .NET.. Язык программирования C#. Основы Web-программирования. Языки сценариев.</p>	
<p><b>Б1.Б.22</b></p>	<p style="text-align: center;"><b>ЭЛЕКТРОНИКА И СХЕМОТЕХНИКА</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целями изучения дисциплины являются: ознакомление студентов с законами преобразования и способами передачи информационных сигналов в электронных устройствах и линиях связи; формирование знаний в области схемотехники аналоговых и цифровых электронных устройств.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Изучение данной дисциплины базируется на знаниях в области дисциплин математического и естественнонаучного цикла: «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Физика», «Информатика».</p> <p>Знания, полученные студентами на курсе «Электроника и схемотехника»,</p>	<p><b>180 (5)</b></p>

	<p>необходимы для освоения дисциплин «Программно-аппаратные средства обеспечения информационной безопасности» и «Разработка и эксплуатация защищенных автоматизированных систем».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-10</b> способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основы теории электрических цепей;</li> <li>- принципы работы элементов и функциональных узлов электронной аппаратуры;</li> <li>- методы анализа и синтеза электронных схем;</li> <li>- типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- применять на практике методы анализа электрических цепей;</li> <li>- работать с современной элементной базой электронной аппаратуры;</li> <li>- применять метод синтеза при разработке электронных схем;</li> <li>- использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры;</li> <li>- навыками работы с программными средствами схемотехнического моделирования;</li> <li>- навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;</li> <li>- навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы;</li> <li>- навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;</li> <li>- быстродействия и оптимизации работы электронных схем на базе современной элементной базы</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Электрические цепи, сигналы. Электрические цепи . Цепи при гармоническом воздействии. Методы анализа сложных электрических цепей.. .  Четырехполюсники, фильтры и длинные линии связи. Сигналы и их спектры..  Полупроводниковые приборы. Электронные усилители и преобразователи сигналов. Нелинейные преобразователи сигналов. Импульсные и цифровые устройства. Цифровая обработка сигналов.</p>	
<p><b>Б1.Б.23</b></p>	<p align="center"><b>БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ</b></p> <p><b>Цели изучения дисциплины:</b>  Дисциплина «Безопасность операционных систем» имеет целью обучить студентов принципам построения защиты информации в ОС и анализа надежности защиты ОС.</p> <p>Задачи дисциплины – дать основы принципов построения подсистем защиты в ОС различной архитектуры; средств и методов несанкционированного доступа к ресурсам ОС; системного подхода к проблеме защиты информации в ОС; механизмов защиты информации и</p>	<p align="center"><b>216 (6)</b></p>

возможностей по их преодолению.

**Место дисциплины в структуре ООП:** Дисциплина «Безопасность сетей ЭВМ» входит в базовую часть профессионального цикла дисциплин СЗ.Б.6 образовательной программы по специальности «Информационная безопасность автоматизированных систем».

Для освоения дисциплины студенты используют знания, умения и компетенции, сформированные в ходе изучения дисциплин «Информатика», «Безопасность сетей ЭВМ», «Сети и системы передачи информации», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем».

Дисциплина является предшествующей для изучения дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем», «Управление информационной безопасностью», «Моделирование угроз информационной безопасности» и др.

**Требования к результатам освоения дисциплины:** процесс изучения дисциплины «Безопасность операционных систем» направлен на формирование следующих компетенций:

К **ПК-23** способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;

К **ПК-25** способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нестандартных ситуаций

**В результате изучения дисциплины студенты должны:**

**знать:**

- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;
- критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.

**уметь:**

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем;
- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; проводить мониторинг угроз безопасности компьютерных сетей/

**владеть:**

- профессиональной терминологией в области информационной безопасности; навыками работы с современными операционными системами, восстановления операционных систем после сбоев;
- установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности;
- 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;
- использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;

**Основные разделы дисциплины:**

	<p>Определение предмета безопасности операционных систем (ОС). Общее понятие безопасности операционных систем, история развития вопроса, характеристика подходов к обеспечению безопасности операционных систем. Операционная система с точки зрения специалиста по информационной безопасности. Общая концепция построения ОС, виды ОС, история развития, семейства ОС. Принципы организации многозадачной ОС. Виды многозадачности, технологии обеспечения многозадачности ОС. Принципы организации межпрограммного взаимодействия. Сетевая подсистема ОС. Принципы построения. Подсистема безопасности ОС. Модели безопасности в различных семействах ОС. Дискреционный и мандатный принципы управления доступом – сравнительный анализ. Многопользовательские ОС. Методы авторизации и аутентификации пользователей. Известные уязвимости. Обеспечение безопасности ОС – журналирование системных событий, системный аудит и анализ инцидентов. Использование средств шифрования в современных ОС. Понятие криптоядра. Сравнительный анализ использования средств шифрования в ОС семейства Microsoft Windows и Linux.</p> <p><b>Общая трудоемкость дисциплины:</b> Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 часов: аудиторные часы – 90 часов, самостоятельная работа – 90 часов, экзамен – 36 часов. Основные виды учебной работы: лекции; практические занятия; СРС. Форма проведения аттестации – зачет, экзамен.</p>	
<p><b>Б1.Б.24</b></p>	<p style="text-align: center;"><b>БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ</b></p> <p><b>Цели изучения дисциплины:</b> Целью преподавания дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей. В результате изучения курса студент должен знать принципы построения и функционирования современных вычислительных сетей, основные сетевые протоколы и технологии обеспечения безопасности в сетях. Студент должен уметь проектировать и администрировать сети с учетом необходимых требований безопасности, используя необходимые программно-аппаратные средства.</p> <p><b>Место дисциплины в структуре ООП:</b> Для освоения дисциплины студенты используют знания, умения и компетенции, сформированные в ходе изучения дисциплин «Информатика», «Физические основы передачи информации», «Сети и системы передачи информации», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем». Знания, полученные студентами при изучении курса необходимы для освоения дисциплин: «Безопасность операционных систем», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем» и др.</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения дисциплины «Безопасность сетей ЭВМ» направлен на формирование следующих компетенций:</p> <p>К <b>ПК-23</b> способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</p> <p>К <b>ПСК-7.1</b> способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p>способностью проводить анализ рисков информационной безопасности и</p> <p><b>ПСК-7.2</b> разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студенты должны:</b></p>	<p><b>252 (7)</b></p>

	<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>К принципы организации, архитектуру и функционирование локальных и корпоративных сетей ЭВМ;</li> <li>К сетевые топологий и методы проектирования сетей ЭВМ;</li> <li>К критерии оценки эффективности и надежности средств защиты операционных систем;</li> <li>К принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>К использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;</li> <li>К проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;</li> <li>К эффективно использовать различные методы и средства защиты информации для компьютерных сетей; проводить мониторинг угроз безопасности компьютерных сетей;</li> <li>К оценивать эффективность и надежность защиты операционных систем.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>К 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;</li> <li>К методами тестирования вычислительных сетей; мониторинга и настройки производительности;</li> <li>К навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;</li> <li>К навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей.</li> </ul> <p><b>Основные разделы дисциплины:</b> Определение предмета безопасности вычислительных сетей Вычислительная сеть с точки зрения специалиста по информационной безопасности Основы сетевой безопасности. Семиуровневая эталонная модель межсетевого взаимодействия (модель OSI) . IP-сети Классификация сетевого оборудования Построение безопасных коммутируемых локальных вычислительных сетей (LAN). Маршрутизация Межсетевое экранирование Системы обнаружения вторжений Виртуальные частные сети. Основные принципы и алгоритмы Беспроводные технологии Глобальные сети и сервисы . Хакеры и методы противодействия хакерам Классификация сетевых атак Принципы построения безопасной вычислительной сети</p>	
<p><b>Б1.Б.25</b></p>	<p style="text-align: center;"><b>БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Безопасность систем баз данных» является изучение реализации политики безопасности баз данных и формирование у студентов навыков ее практического применения в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Безопасность систем баз данных» рассматривает основные принципы и основные направления обеспечения безопасности данных.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Безопасность систем баз данных» входит в цикл дисциплин Б1.Б.25 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Успешное усвоение материала предполагает знание студентами основных</p>	<p><b>216 (6)</b></p>



положений курсов «Информатика», «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Основы информационной безопасности», «Информационные технологии. Базы данных».

Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ПК-23** - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;

**ПК-25** - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;

**ПСК-7.1** - способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;

**ПСК-7.2** - способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах.

**В результате изучения дисциплины студент должен:**

**знать:**

- Принципы формирования политики информационной безопасности автоматизированных систем;
- Организацию автоматизированной системы с учетом требований информационной безопасности;
- Стратегию развития информационного общества в России;
- Организацию защиты информации баз данных;
- Сравнительный анализ эффективности применения средств обеспечения безопасности данных.

**уметь:**

- Организовывать безопасность систем баз данных;
- Эффективно применять средства обеспечения безопасности данных;
- Анализировать стратегию развития информационного общества в России;
- Самостоятельно организовывать эксплуатацию автоматизированной системы с учетом требований информационной безопасности;
- Участвовать в формировании политики информационной безопасности автоматизированных систем.

**владеть:**

- Основными принципами формирования политики информационной безопасности автоматизированных систем;
- Методами и средствами программно-аппаратной защиты информации для организации защищенной автоматизированной системы с учетом требований информационной безопасности;
- Навыками анализа методов формирования требований по защите информации;
- Навыками организации безопасности систем баз данных. Средствами обеспечения безопасности данных и АИС.

**Дисциплина включает в себя следующие разделы:**

Общие положения обеспечения безопасности доступа к данным. Обеспечение

	надежной аутентификации. Управление доступом к данным. Парольные политики. Документирование баз данных с учетом требований по обеспечению информационной безопасности. Атаки на системы данных. Применение средств криптографической защиты информации (СКЗИ). СКЗИ «Крипто БД».	
<b>Б1.Б.26</b>	<p style="text-align: center;"><b>ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p>Цель изучения дисциплины:  понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной безопасности Российской Федерации. Формирование у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации.</p> <p>Изучение дисциплины базируется на знаниях, умениях и навыках, полученных в результате освоения дисциплины «Основы управленческой деятельности».</p> <p>Знания и умения, полученные студентами при изучении дисциплины, необходимы для изучения «Организационно – правовое обеспечение информационной безопасности», «Информационная безопасность распределенных ИС», «Методы проектирования распределенных приложений».</p> <p>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности</li> <li>– ПК-3 способностью проводить анализ защищенности автоматизированных систем</li> <li>– ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению</li> <li>– ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности</li> </ul> <p>В результате изучения дисциплины обучающийся должен:</p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>– Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ.</li> <li>– Современные способы использования компьютерных технологий для проведения исследований.</li> <li>– Технические средства контроля эффективности мер защиты информации</li> <li>– Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем</li> <li>– Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах.</li> <li>– Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>– Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.</li> <li>– Анализировать основные узлы и устройства современных</li> </ul>	108(3)

	<p>автоматизированных систем</p> <ul style="list-style-type: none"> <li>– Эффективно использовать современные компьютерные технологии для изучения предмета исследования.</li> <li>– Анализировать современную научно-техническую информацию по информационной безопасности.</li> <li>– Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе</li> <li>– Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– Методами разработки проектов нормативных документов, регламентирующих работу по защите информации</li> <li>– Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.</li> <li>– Навыками анализа защищенности информационной инфраструктуры автоматизированной системы</li> <li>– Профессиональной терминологией в области информационной безопасности.</li> <li>– Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах</li> <li>– Методами синтеза структурных и функциональных схем защищенных автоматизированных систем</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Место и роль информационной безопасности в системе национальной безопасности РФ.  Классификация защищаемой информации и угроз информационной безопасности  Способы обеспечения информационной безопасности автоматизированных систем.  Методы формирования требований по защите информации АС.</p>	
<p><b>Б1.Б.27</b></p>	<p><b>КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Криптографические методы защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Задачами изучения дисциплины является изложение студентам основ системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе.</p> <p><b>Задачами изучения дисциплины являются:</b></p> <ol style="list-style-type: none"> <li>1. получение знаний по: основным понятиям криптографии; моделям шифров и математическим методам их исследования; требованиям, предъявляемым к шифрам и основным характеристикам шифров; основополагающим принципам защиты информации на основе криптографических методов; криптографическим стандартам и их использовании в информационных системах;</li> <li>2. приобретение умений по реализации криптографических методов на практике;</li> <li>3. приобретение навыков: владения криптографической терминологией; использования типовых криптографических алгоритмов; использование ПЭВМ в анализе простейших шифров.</li> </ol>	<p><b>252 (7)</b></p>

	<p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Криптографические методы защиты информации» формирует профессиональные знания, необходимые для будущей трудовой деятельности. Успешное усвоение материала предполагает знание студентами основных положений курсов «Основы информационной безопасности», «Математическая логика и теория алгоритмов», «Информатика», «Математический анализ», «Программно-аппаратные средства обеспечения информационной безопасности», «Технологии и методы программирования», «Языки программирования».</p> <p>Компетенции, полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Алгоритмы шифрования информации».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-14</b> - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- Способы контрольных проверок работоспособности и эффективности применяемых криптографических средствЗИ.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- Навыками анализа архитектурно технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Введение в криптографию. Основные классы шифров и их свойства. Принципы построения криптографических алгоритмов Реализация криптографических алгоритмов.</p>	
<p><b>Б1.Б.28.</b></p>	<p><b>ОРГАНИЗАЦИЯ ЭВМ И ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целями освоения дисциплины «Организация ЭВМ и вычислительных систем» является формирование у студентов понятий об основных принципах организации технических средств ЭВМ и систем; о функциональной и структурной организации ЭВМ; о принципах построения основных устройств ЭВМ; об важнейших этапах и тенденциях в развитии цифровой, аналоговой и гибридной вычислительной техники; о методах оценки параметров ЭВМ и отдельных их устройств и овладение студентами необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВПО для специальности <i>10.05.03 Информационная безопасность автоматизированных систем.</i></p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Для усвоения данной дисциплины студенту необходим объём знаний,</p>	<p><b>108(3)</b></p>

	<p>предусмотренный курсами информатики, физики общеобразовательной школы (элементарные знание дискретной математики, систем исчисления, базовые представления об электромагнитном взаимодействии).</p> <p>Данная дисциплина необходима для последующего успешного освоения следующих дисциплин: «Электроника и схемотехника», «Сети и системы передачи информации», «Техническая защита информации», «Безопасность сетей ЭВМ».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-9.</b> Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>ПСК-7.4.</b> Способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <p>Логику работы центрального процессора при выполнении вычислений и при передаче данных между ЦП и периферийными устройствами ПК</p> <p>Особенности удалённого администрирования различных операционных систем</p> <p><b>уметь:</b></p> <p>Проектировать одноранговые вычислительные сети</p> <p>Управлять процессами, происходящими на удаленной рабочей станции или сервере баз данных</p> <p><b>владеть навыками:</b></p> <p>Навыками работы с пакетами моделирующими работу вычислительных сетей</p> <p>Способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>История развития вычислительной техники. Представление информации в вычислительных системах. Архитектура и принципы работы основных логических блоков ЭВМ. Организация работы памяти ЭВМ. Внутренние интерфейсы ЭВМ. Информационные сети. Операционные системы ЭВМ.</p>	
<p><b>Б1.Б.29</b></p>	<p style="text-align: center;"><b>ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Техническая защита информации» является формирование профессиональных навыков обеспечения информационной защиты от съема информации по техническим каналам утечки информации, использования методов и средств инженерно-технической защиты информации и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Техническая защита информации» рассматривает основные принципы и основные направления технической защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Техническая защита информации» входит в цикл дисциплин Б1.Б.29 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Успешное усвоение материала предполагает знание студентами основных положений курсов «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Физика», «Основы радиотехники», «Теория информации», «Основы информационной безопасности», «Электроника и схемотехника». Дисциплина является предшествующей для изучения дисциплин:</p>	<p><b>216 (6)</b></p>

	<p>«Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-14</b> - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p> <p><b>ПК-17</b> - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.</li> <li>- Организацию защиты информации от утечки по техническим каналам на объектах информатизации.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.</li> <li>- Применять технические средства обеспечения информационной безопасности.</li> <li>- Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- Методами и средствами технической защиты информации.</li> <li>- Навыками анализа архитектурно-технических и схмотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>          Электромагнитный канал утечки информации. Оптический канал утечки информации. Электросетевой канал утечки информации. Поиск средств несанкционированного съема информации.</p>	
<p><b>Б1.Б.30</b></p>	<p align="center"><b>СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ</b></p> <p><b>Цель дисциплины:</b> изучение структуры локальных и глобальных сетей и систем передачи информации; освоение методов настройки и работы в сетях и системах передачи информации.</p> <p><b>Место дисциплины в структуре ООП:</b>          Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате изучения предмета «Информатика и информационно-коммуникационные технологии» в объеме средней общеобразовательной школы и предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем». Знания, умения и навыки, полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Виртуальные сети», «Безопасность сетей ЭВМ», «Методы проектирования защищенных распределенных информационных систем», «Информационная безопасность распределенных информационных систем».</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения дисциплины «Сети и системы передачи информации» направлен на формирование следующих компетенций:</p>	<p><b>144 (4)</b></p>

	<p><b>ПК-10</b> -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</p> <p><b>ПСК-7.4</b> - способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студенты должны:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>К Основные формальные модели управления доступом в сетях и системах передачи информации.</li> <li>К Типовые структуры и принципы организации компьютерных сетей.</li> <li>К Методы и средства получения, обработки и передачи информации в современных операционных системах и компьютерных сетях.</li> <li>К Методы и средства защиты информации в компьютерных сетях и операционных системах.</li> <li>К Принципы построения современных операционных систем и особенности их применения для решения задач защиты информации в сетях.</li> <li>К Основные виды политик управления доступом и информационными потоками в сетях.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>К Формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.</li> <li>К Проводить анализ показателей качества сетей и систем связи.</li> <li>К Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>К Навыки обеспечения безопасности информации с помощью стандартных сетевых средств обмена информацией.</li> <li>К Оценкой технико-экономический уровня и эффективности предлагаемых и реализуемых технических решений в сетях и системах передачи информации.</li> <li>К Устанавливать и настраивать программное обеспечение, необходимое для администрирования в сетях.</li> </ul> <p><b>Основные (разделы):</b> Принципы построения и функционирования локальных и глобальных сетей, систем передачи информации. Понятие локальных и глобальных сетей. Общие понятия и принципы функционирования сетей. Топология сетей. эталонная модель взаимодействия открытых систем ISO/OSI. Общие сведения о протоколах эталонной семиуровневой модели. Особенности современных сетевых архитектур локальных сетей. Протоколы физического и канального уровней модели взаимодействия открытых систем. Основы физической коммутации витой пары и оптоволокна. Методы коммутации информации; особенности сетей с коммутацией каналов, сообщений и пакетов; технические характеристики и принципы функционирования современных модемов. Маршрутизация и управление потоками в сетях связи; сети интегрального обслуживания. Классификация систем связи; кодирование информации в системах связи. Методы модуляции в системах связи; основные типы модемов; уплотнение информации в системах связи; цифровая обработка аналоговых сигналов. Системы телефонной связи; цифровая телефония; системы телеграфной связи; коротковолновые и ультракоротковолновые системы связи; радиорелейные системы связи; телевизионные системы; спутниковые системы связи; волоконно-оптические системы связи. Современные операционные системы и их применение для защиты информации в сетях. Современные системы передачи данных.</p>	
Б1.Б.31	<b>ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ</b>	<b>108(3)</b>

## **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **Цели изучения дисциплины:**

Целями освоения являются: обучить студентов 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.

Задачи дисциплины: дать представление о законодательстве РФ в области информации; ознакомить с системой защиты государственной тайны; ознакомить с правилами лицензирования и сертификации в области защиты информации; ознакомить с организационными методами защиты информации; ознакомить с методами обеспечения информационной безопасности.

### **Место дисциплины в структуре ООП:**

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин: «Основы информационной безопасности», «Введение в специальность».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Основы управленческой деятельности», «Управление информационной безопасностью».

### **Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

ОК 4 способностью использовать основы правовых знаний в различных сферах деятельности

ОПК 6 способностью использовать нормативные правовые акты в своей профессиональной деятельности

ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

### **В результате изучения дисциплины студент должен:**

#### **знать:**

- основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
- 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;
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности



	<p>автоматизированных систем;</p> <ul style="list-style-type: none"> <li>- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;</li> <li>- методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;</li> <li>- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);</li> <li>- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</li> <li>- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками работы с нормативными правовыми актами;</li> <li>- навыками организации и обеспечения режима секретности;</li> <li>- методами организации и управления деятельностью служб защиты информации на предприятии;</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>          Основы законодательства Российской Федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты информации. Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Лицензирование в области защиты информации. Сертификация в области защиты информации. Защита интеллектуальной собственности. Организационное обеспечение информационной безопасности. Анализ и оценка угроз информационной безопасности объекта. Средства и методы физической защиты объекта. Организация и обеспечение режима секретности.</p>	
<p><b>Б1.Б.32</b></p>	<p align="center"><b>ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является формирование профессиональных навыков администрирования подсистем информационной безопасности автоматизированной системы и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных программно-аппаратных СЗИ в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» рассматривает базовые теоретические понятия, лежащие в основе программно-аппаратной защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» входит в цикл дисциплин Б1.Б.32 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Успешное усвоение материала</p>	<p align="center"><b>180 (5)</b></p>

предполагает знание студентами основных положений курсов «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Информатика», «Основы радиотехники», «Теория информации», «Основы информационной безопасности», «Технологии и методы программирования». Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ОПК-8** - способностью к освоению новых образцов программных, технических средств и информационных технологий.

**ПК-10** - способностью применять знания в области электроники и схмотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности.

**ПК-14** - способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

**ПК-26** - способностью администрировать подсистему информационной безопасности автоматизированной системы.

**В результате изучения дисциплины студент должен:**

**знать:**

- Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных средств ЗИ.
- Принципы администрирования системы информационной безопасности автоматизированной системы.
- Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.
- Типовые структуры и принципы организации программных и программно-аппаратных средств ЗИ.

**уметь:**

- Эффективно использовать и оптимизировать свою работу за счет использования новых программных и технических средств и информационных технологий.
- Анализировать программные, архитектурно-технические и схмотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.
- Применять программные и программно-аппаратные средства обеспечения ИБ.
- Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных средств обеспечения информационной безопасности.
- Самостоятельно администрировать систему информационной безопасности автоматизированной системы.

**владеть:**

- Навыками администрирования системы информационной безопасности автоматизированной системы.
- Навыками анализа архитектурно-технических и схмотехнических решений компонентов автоматизированных систем с целью выявления потенциальных

	<p>уязвимостей информационной безопасности автоматизированных систем.</p> <ul style="list-style-type: none"> <li>- Навыками анализа программных, архитектурно-технических и схемотехнических решении компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.</li> <li>- Навыками повышения эффективности работы с использованием информационных технологий.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Общие положения защиты информации программно-аппаратными средствами. Задачи и методы защиты информации от НСД. СЗИ от НСД «СТРАЖ NT». Обеспечение разграничения и контроля доступа пользователей различными способами.</p>	
<p><b>Б1.Б.33</b></p>	<p style="text-align: center;"><b>РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ</b></p> <p><b>Цель изучения дисциплины:</b>  обучить студентов методическим вопросам оценки эффективности сложных систем, принципам хранения, обработки и передачи информации в автоматизированных системах, обратить внимание на вопросы безопасного функционирования автоматизированной системы. Знания и практические навыки, полученные в курсе “Разработка и эксплуатация защищенных автоматизированных систем” используются обучаемыми при разработке курсовых и дипломных работ. Задачи дисциплины: основы построения и эксплуатации систем контроля доступа системного подхода к проблеме защиты информации в автоматизированных системах, механизмов защиты информации и возможностей по их преодолению; изучение принципов организации и структуру систем защиты информации автоматизированных систем.</p> <p>Изучение дисциплины базируется на знаниях, умениях и навыках, полученных в результате освоения <b>дисциплин</b> «Теория вероятностей, математическая статистика», «Основы информационной безопасности», «Безопасность сетей ЭВМ», «Безопасность систем баз данных», «Введение в специальность».</p> <p>Знания и умения, полученные студентами при изучении дисциплины, <b>необходимы для изучения дисциплин «Информационная безопасность распределенных информационных систем» «Методы проектирования защищенных распределенных информационных систем», «Моделирование систем и процессов защиты информации», «Управление информационной безопасностью».</b>  Изучение дисциплины направлено на формирование и развитие следующих компетенций:</p> <ul style="list-style-type: none"> <li>– <b>ПК-9</b> способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</li> <li>– <b>ПСК-7.2.</b> – способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах</li> </ul> <p><b>В результате изучения дисциплины обучающийся должен:</b>  <b>знать:</b></p> <ul style="list-style-type: none"> <li>– Основные характеристики технических средств защиты информации от утечек по техническим каналам</li> <li>– Принципы формирования политики информационной безопасности в автоматизированных системах</li> <li>– Принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем</li> </ul>	<p>324(9)</p>

	<p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>– Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем</li> <li>– Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– Приемами разработки моделей автоматизированных систем и подсистем безопасности автоматизированных систем</li> <li>– Приемами разработки проектов нормативных документов, регламентирующих работу по защите информации</li> <li>– Навыками разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем; разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах</li> <li>– Принципами формирования политики информационной безопасности в автоматизированных системах</li> </ul> <p>Дисциплина включает в себя следующие разделы:</p> <ol style="list-style-type: none"> <li>1. Теоретические основы построения и эксплуатации АС</li> <li>2. Архитектура защищенных систем.</li> <li>3. Реализация механизмов безопасности АС.</li> </ol>	
<p><b>Б1.Б.34</b></p>	<p align="center"><b>УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целями изучения дисциплины «Управление информационной безопасностью» являются: формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих и государственных организациях РФ; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих, государственных организациях и организациях банковской системы РФ; развитие способностей по использованию существующей системы управления информационной безопасности.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Управление информационной безопасностью» входит в цикл Б1.Б.32 образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем».</p> <p>Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Основы управленческой деятельности», «Разработка и эксплуатация защищенных автоматизированных систем».</p> <p>Компетенции, приобретенные в процессе изучения данной дисциплины, будут необходимы для выполнения выпускной квалификационной работы.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-12</b> - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы.</p> <p><b>ПК-11</b> - способностью разрабатывать политику информационной</p>	<p><b>288 (8)</b></p>

	<p>безопасности автоматизированной системы.</p> <p><b>ПК-19</b> - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы.</p> <p><b>ПК-28</b> - способностью управлять информационной безопасностью автоматизированной системы.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- Место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России.</li> <li>- Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</li> <li>- Сущность и понятие информации, информационной безопасности и характеристику ее составляющих.</li> <li>- Основные подходы к проектированию систем управления информационной безопасностью автоматизированной системы.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, - разрабатывать модели систем организационного управления.</li> <li>- Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.</li> <li>- Разрабатывать частные политики информационной безопасности автоматизированных систем, контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем</li> <li>- Проводить аудит ИБ (комплексное диагностическое обследование ИБ) и разрабатывать сопроводительную документацию.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- Навыками сбора данных и описания текущего состояния системы ИБ и определения критериев защищенности информационной системы с целью разработки требований к разрабатываемым процессам управления.</li> <li>- Навыками разработки политики безопасности систем организационного управления.</li> <li>- Методами управления информационной безопасностью автоматизированных систем.</li> <li>- Методами управления ИБ автоматизированных систем, навыками разработки политики безопасности систем организационного управления.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Основные задачи управления информационной безопасностью Основные составляющие информационной безопасности. Аудит систем управления ИБ.</p>	
<p><b>Б1.Б.35</b></p>	<p style="text-align: center;"><b>ИНЖЕНЕРНАЯ ГРАФИКА</b></p> <p><b>Цели изучения дисциплины:</b>  Цель обучения инженерной графике - овладение студентами знаниями, умениями и навыками, необходимыми для выполнения и чтения чертежей различного назначения и решения на чертежах инженерно-графических задач. Овладение чертежом как средством выражения технической мысли и как производственным документом осуществляется на протяжении всего процесса обучения в университете. Этот процесс начинается с изучения основ начертательной геометрии в курсе инженерной графики, а затем развивается и закрепляется в ряде специальных дисциплин, а также при выполнении</p>	<p><b>108 (3)</b></p>

курсовых работ и дипломного проекта. Также целью изучения инженерной графики является овладение решением задач геометрического моделирования и применения интерактивных графических систем для выполнения и редактирования изображений и чертежей (с помощью компьютерных графических пакетов).

Указанная цель достигается за счет развития пространственного видения студентов, необходимого для специальных технических дисциплин и в последующей профессиональной деятельности, обучения теоретическим основам проецирования, способам построения изображения деталей и их соединений в соответствии со стандартами ЕСКД.

#### **Место дисциплины в структуре ООП:**

Для усвоения Инженерной графики студенту необходим объем знаний, предусмотренный курсами геометрии, черчения, информатики общеобразовательной школы (знания об элементарных геометрических объектах (точка, прямая, кривая, плоскость, поверхность), о взаимном положении (параллельность, пересечение, перпендикулярность), о разновидностях кривых (окружность, эллипс, гипербола, парабола); виды поверхностей – призма, пирамида, цилиндр, конус, сфера); умение изобразить перечисленные геометрические объекты на одной плоскости; иметь: навыки выполнения чертежей геометрических моделей на трех плоскостях проекций; начальные навыки работы с компьютером.

Данная дисциплина необходима для последующего успешного освоения следующих дисциплин: «Техническая защита информации», «Методы проектирования защищенных распределенных информационных систем», в рамках оформления технической документации.

#### **Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ОПК-5** способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами

#### **В результате изучения дисциплины студент должен:**

##### **знать:**

- основные определения и понятия начертательной геометрии и технического черчения.
- способы построения изображений пространственных форм в ортогональных и изометрических проекциях
- способы решения задач, относящихся к этим формам: метрических и позиционных;
- основы начертательной геометрии: способы проецирования, методы построения чертежей трехмерных объектов; основы инженерной графики: теоретические основы и правила построения изображений.

##### **уметь:**

- использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;
- применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;
- создавать конструкторскую документацию в соответствии с требованиями стандартов ЕСКД
- пользоваться измерительными инструментами;
- читать чертежи и выполнять построения технических изделий;
- представлять технические решения с использованием средств компьютерной графики и геометрического моделирования;
- пользоваться учебной и справочной литературой, стандартами ЕСКД, измерительными инструментами, решать позиционные и метрические задачи; строить изображения технических изделий на комплексных и

	<p>аксонометрических чертежах; выполнять эскизы деталей машин; изображать, сборочные чертежи изделий;</p> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации.</li> <li>- работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;</li> <li>- методами и приемами изображения пространственных объектов на плоских чертежах.</li> <li>- разработки и оформления чертежей (эскизов деталей, изображения сборочных единиц, сборочного чертежа изделия) с использованием современных графических редакторов и пакетов прикладных программ по проектированию.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Предмет инженерной и компьютерной графики. Стандарты ЕСКД. ГОСТ ы 2.301-68 – 2.307-68, ГОСТ 2.305-68. Основы начертательной геометрии. Способы проецирования. Плоскость. Многогранники. Кривые поверхности. Поверхности вращения. Образование. Изображение окружности, плоских фигур. ЕСКД. ГОСТ 2.317-69. Сечение поверхностей проецирующей плоскостью. Компьютерная графика. Основные операции в пакетах прикладных программ для выполнения чертежей и проектной документации. Выполнение чертежей средствами компьютерной графики и САПР. Основы инженерной графики. Правила оформления конструкторской документации в соответствии с действующими нормативами. Разъемные и неразъемные соединений. Эскизирование деталей машин.</p>	
<p><b>Б1.Б.36</b></p>	<p align="center"><b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Информационная безопасность распределенных информационных систем» является формирование 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. Овладение обучающимися необходимым и достаточным уровнем компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Для усвоения данной дисциплины обучающемуся необходим объём знаний, предусмотренный курсами информатики, организации ЭВМ и вычислительных систем, технологии и методы программирования, языки программирования, сети и системы передачи информации, технологии построения защищенных распределенных приложений, методы проектирования защищенных распределенных информационных систем и т.д. Данная дисциплина необходима для последующего успешного выполнения научно-исследовательской работы.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p>	<p><b>144 (4)</b></p>

**ПК-3** - Способностью проводить анализ защищенности автоматизированных систем;

**ПК-20** - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

**ПК-27** - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;

**ПСК-7.5** - способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении.

**В результате изучения дисциплины студент должен:**

**знать:**

- Способы анализа эффективности координирования деятельности подразделений по защите информации на предприятии, в учреждении, организации;
- Способы управления разработкой политики безопасности распределенных информационных систем.
- Методы и средства анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации защищенных распределенных автоматизированных систем;
- Нормативные методические документы ФСБ РФ и ФСТЭК РФ в области защиты информации.
- Методики проектирования АС в защищенном исполнении;
- Методики анализа и контроля защищенности распределенных информационных систем в защищенном исполнении.

**уметь:**

- Проводить выбор технических, программно-аппаратных компонентов автоматизированных систем с целью совершенствования защиты;
- Организовывать реализацию разработанной автоматизированной системы с учетом требований информационной безопасности. Готовить сопроводительную документацию к разработанной АС в защищенном исполнении;
- Осуществлять контроль эффективности применения разработанной АС в защищенном исполнении;
- Руководить разработкой и реализацией частных политики безопасности распределенных информационных систем;
- Осуществлять мониторинг и аудит безопасности автоматизированной системы;
- Совершенствовать существующий подход координации деятельности подразделений по защите информации на предприятии, в учреждении, организации.

**владеть:**

- Методиками анализа эффективности руководства подразделений по защите информации на предприятии, в учреждении, организации;
- Методиками руководства разработкой политики безопасности распределенных информационных систем;
- Методами обеспечения требований по информационной безопасности процессов создания и эксплуатации защищенных распределенных АС;
- Навыками контроля реализации политики информационной безопасности;
- Навыками контроля эффективности применения разработанной АС в защищенном исполнении.
- Навыками разработки сопроводительной документации к разработанной АС



	<p>в защищенном исполнении; - Методами и технологиями проектирования, моделирования, исследования автоматизированных систем в защищённом исполнении.</p> <p><b>Дисциплина включает в себя следующие разделы:</b> Распределенные информационные системы: основные понятия. Автоматизированные системы и их связь с информационной безопасностью распределенных информационных систем. Коммуникация в распределенных информационных системах, проектирование системы защиты информации в распределенных информационных системах.</p>	
<p><b>Б1.Б.37</b></p>	<p style="text-align: center;"><b>МЕТОДЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ</b></p> <p><b>Цели изучения дисциплины:</b> Целями изучения дисциплины «Методы проектирования защищенных распределенных информационных систем» являются: изучение технологий проектирования защищенных распределенных информационных систем, различных подходов к проектированию с применением современных CASE-средств, знакомство с современными подходами к проектированию, эксплуатации и модернизации информационных систем.</p> <p><b>Место дисциплины в структуре ООП:</b> В результате изучения дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Технология построения защищенных распределенных приложений». Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: «Информационная безопасность распределенных информационных систем», «Моделирование систем и процессов защиты информации».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ПК-6</b> способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности <b>ПК-8</b> способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем <b>ПК-15</b> способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b> - принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования</p> <p><b>уметь:</b> - использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.</p> <p><b>владеть навыками:</b> - навыками семантического моделирования данных, навыками</p>	<p><b>144 (4)</b></p>

	<p>проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения.</p> <p><b>Дисциплина включает в себя следующие разделы:</b>          Теоретические основы проектирования информационных систем. Технологии проектирования ИС. Стандарты и профили в области информационных систем. Моделирование функциональной области внедрения ИС.          Автоматизированное проектирование ИС. Типовое проектирование ИС.          Проектирование процессов защиты данных. Управление проектированием ИС.</p>	
<p><b>Б1.Б.38</b></p>	<p style="text-align: center;"><b>ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ПРИЛОЖЕНИЙ</b></p> <p><b>Цели изучения дисциплины:</b>          Целями освоения дисциплины «Технология построения защищенных распределенных приложений» является формирование у студентов понятий о современных подходах к проектированию и построению, эксплуатации и модернизации защищенного программного обеспечения в целом, формирует у студентов 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 студентов практические навыки использования CASE-средств для построения и модернизации программного обеспечения.          Овладение студентами необходимым и достаточным уровнем общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности <i>10.05.03 Информационная безопасность автоматизированных систем</i>.</p> <p><b>Место дисциплины в структуре ООП:</b>          Для усвоения данной дисциплины студенту необходим объём знаний, предусмотренный курсами информатики, организации ЭВМ и вычислительных систем, технологии и методы программирования, языки программирования, сети и системы передачи информации.          Данная дисциплина необходима для последующего успешного освоения следующих дисциплин: «Информационная безопасность распределенных информационных систем», «Методы проектирования защищенных распределенных информационных систем».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ПК-13.</b> Способностью участвовать в проектировании средств защиты информации автоматизированной системы</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b>          Основные способы защиты элементов распределённого приложения          Стандартный алгоритм разработки распределённого приложения</p> <p><b>уметь:</b>          Применять современные способы защиты информации передаваемой по каналу связи          Применять при разработке элементов распределённого приложения параллельные вычисления</p> <p><b>владеть навыками:</b>          Способностью участвовать в проектировании средств защиты информации автоматизированной системы          Методиками защиты информации при ее передаче между элементами распределенной системы</p> <p><b>Дисциплина включает в себя следующие разделы:</b>          Введение в распределенные приложения. Взаимодействие компонент</p>	<p><b>108(3)</b></p>

	<p>распределенного приложения. Описание интерфейса программной компоненты. Сериализация объектов. Службы обмена сообщениями. Очереди сообщений.</p>	
<p><b>Б1.Б.39</b></p>	<p style="text-align: center;"><b>ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ</b></p> <p>Цель изучения дисциплины:  ознакомление студентов с профессиональной деятельностью в сфере разработки, исследования и эксплуатации систем обеспечения информационной безопасности автоматизированных систем в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Введение в специальность» содействует формированию мировоззрения и системного мышления, ориентирует обучающихся в широкой сфере проблем обеспечения информационной безопасности автоматизированных систем</p> <p>Изучение дисциплины базируется на знаниях, умениях и навыках, полученных в результате освоения <b>дисциплин</b> «Информатика и информационно-коммуникационные технологии», «Алгебра» и «Физика» в объеме средней общеобразовательной школы.</p> <p>Знания и умения, полученные студентами при изучении дисциплины, <b>необходимы для изучения дисциплин</b> «Основы информационной безопасности», «Управление информационной безопасностью» «Моделирование угроз информационной безопасности», «Моделирование систем и процессов защиты информации».</p> <p>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</p> <ul style="list-style-type: none"> <li>– <b>ОК-5</b> - способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</li> <li>– <b>ПК-1</b> - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</li> </ul> <p>В результате изучения дисциплины обучающийся должен:</p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>– Формы и способы представления данных в персональном компьютере.</li> <li>– Особенности обработки информации с использованием компьютерных систем</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>– Эффективно использовать найденные методики изучения предмета исследования</li> <li>– Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– Навыками повышения эффективности использования информационных технологий для самостоятельной научной и исследовательской работы в профессиональной деятельности</li> <li>– Основными методами научного познания в области защиты информации автоматизированных систем, а так же их применения к решению прикладных задач</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>4. Организация высшего образования в области информационной безопасности</p>	<p><b>72(2)</b></p>

	<ol style="list-style-type: none"> <li>5. Место специальности в системе национальной безопасности РФ</li> <li>6. Способы обеспечения информационной безопасности автоматизированных систем.</li> <li>7. Информационный обзор по вопросам информационной безопасности автоматизированных систем.</li> <li>8. Обобщение научно-технической литературы, нормативных и методических материалов по программно-аппаратным средствам и способам обеспечения информационной безопасности автоматизированных систем.</li> <li>9. Методы и средства, применяемые для контроля и защиты информации.</li> <li>10. Опыт работы учреждений, организаций и предприятий по способам обеспечения информационной безопасности автоматизированных систем</li> <li>11. Выбор оптимального решения по уровню информационной безопасности как компромисса между различными требованиями (безопасности, качества разработки, стоимости и сроков исполнения). Организация работы профессионального коллектива исполнителей, принятие управленческих решений.</li> </ol>	
<p><b>Б1.Б.40</b></p>	<p style="text-align: center;"><b>ФИЗИЧЕСКАЯ КУЛЬТУРА</b></p> <p><b>Цели изучения дисциплины:</b>  Целью физического воспитания студентов вузов является формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности</p> <p>Изучение дисциплины направлено на формирование мотивационно – ценностного отношения к физической культуре, установке на здоровый стиль жизни, физическое совершенствование и самовоспитание привычки к регулярным занятиям физическими направлениями и спортом.</p> <p><b>Место дисциплины в структуре ООП:</b>  Дисциплина «Физическая культура» относится к базовой части Физическая культура. Для освоения дисциплины используются знания, умения и навыки, сформированные в процессе изучения предметов «Культурология», «Психология и педагогика», «Физическая культура» на предыдущем уровне образования.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b>  <b>ОК-9</b> способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- определения и названия основных процессов воспитательной и образовательной деятельности;</li> <li>- нормы здорового образа жизни, ценности физической культуры, способы физического совершенствования организма, основы теории и методики обучения базовым видам физкультурно-спортивной деятельности; содержание, формы и методы организации учебно-тренировочной и соревновательной работы; медико-биологические и психологические основы физической культуры; систему самоконтроля при занятиях физкультурно-спортивной деятельностью; правила личной гигиены; технику безопасности при занятиях физкультурно-спортивной деятельностью.</li> <li>- основные средства и методы воспитательной и образовательной деятельности.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- грамотно применять на практике основные определения физической</li> </ul>	<p><b>72(2)</b></p>

	<p>культуры и укрепления здоровья; правильно организовать режим времени, приводящий к здоровому образу жизни;</p> <ul style="list-style-type: none"> <li>- использовать накопленные в области физической культуры и спорта духовные ценности, для воспитания патриотизма, формирование здорового образа жизни, потребности в регулярных физкультурно-спортивных занятиях; определять цели и задачи физического воспитания, спортивной подготовки и физкультурно-оздоровительной работы, как факторов гармонического развития личности, укрепления здоровья человека; правильно оценивать свое физическое состояние; использовать технические средства и инвентарь для повышения эффективности физкультурно-спортивных занятий; регулировать физическую нагрузку;</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- разнообразными средствами физической культуры, используя различные методы укрепления здоровья;</li> <li>- навыками физических упражнений, физической выносливости, подготовленности организма серьезным нагрузкам в экстремальных ситуациях, средствами и методами физкультурно-спортивной деятельности.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b> Средства, методы и организация физической и спортивной подготовки студента по видам спорта. Баскетбол. Легкая атлетика. Тяжелая атлетика. Футбол. Гимнастика. ОФП. Спецмедотделение.</p>	
<b>Б1.В</b>	<b>ВАРИАТИВНАЯ ЧАСТЬ</b>	
<b>Б1.В.ОД</b>	<b>ОБЯЗАТЕЛЬНЫЕ ДИСЦИПЛИНЫ</b>	
<b>Б1.В.ОД.1</b>	<p><b>ИНОСТРАННЫЙ ЯЗЫК В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины являются: повышение исходного уровня владения иностранным языком и овладение студентами необходимым и достаточным уровнем коммуникативной компетенции для решения социально-коммуникативных задач в различных областях бытовой, культурной, профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.</p> <p><b>Место дисциплины в структуре ООП:</b> Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплины «Иностранный язык». Дисциплина является предшествующей для изучения дисциплин профессионального цикла, использующих терминологию иностранных языков.</p> <p>Знания, умения и навыки, полученные при изучении дисциплины «Иностранный язык в профессиональной деятельности» позволят студентам интегрироваться в международную профессиональную среду и использовать иностранный язык как средство межкультурного и профессионального общения.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-7</b> 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 <b>ПК-1</b> способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</p> <p><b>В результате изучения дисциплины студент должен:</b></p>	<b>144 (4)</b>

	<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке;</li> <li>- функциональные особенности устных и письменных профессионально-ориентированных текстов, в том числе научно-технического характера</li> <li>- функциональные особенности устных и письменных профессионально-ориентированных текстов, в том числе научно-технического характера;</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи;</li> <li>- осуществлять устную и письменную коммуникацию в целях научного академического и коммерческого общения на таких мероприятиях, как доклад на конференции, презентация, дебаты, круглый стол, выставки, реклама и пр.) на иностранном языке;</li> <li>- работать с аутентичной литературой профессионально ориентированного характера и обрабатывать полученную информацию;</li> </ul> <p>понимать устную монологическую и диалогическую речь на профессиональную тематику.</p> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке;</li> <li>- грамматическими навыками, обеспечивающими коммуникацию без искажения смысла при письменном и устном общении;</li> <li>- способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков;</li> <li>- навыками обработки большого объема иноязычной информации с целью сбора материала для написания магистерской диссертации или её раздела на изучаемом языке.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Профессиональная сфера общения. Моя будущая специальность. Направление профессиональной деятельности. Изучаемые дисциплины. История, современное состояние и перспективы развития науки и техники. Предпосылки и последствия научных открытий и изобретений. Экономика в нашей жизни. Сфера профессиональной деятельности. Развитие и перспективы. Информационная безопасность автоматизированных систем. Защищенные автоматизированные системы управления. Автоматизированные информационные системы специального назначения. Высокопроизводительные вычислительные системы специального назначения. Безопасность открытых информационных систем.</p>	
<p><b>Б1.В.ОД.2</b></p>	<p align="center"><b>ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. БАЗЫ ДАННЫХ</b></p> <p><b>Цели освоения дисциплины</b></p> <p>Целью является знакомство с моделями данных, используемыми в СУБД, изучение основ теории реляционных баз данных и методов проектирования баз данных, и формировании у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО для специальности «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.</p>	<p align="center"><b>180 (5)</b></p>

### **Место дисциплины в структуре ООП подготовки специалиста**

Дисциплина «Информационные технологии. Базы данных» относится к вариативной части математического и естественнонаучного цикла дисциплин: С2.В.ОД.1.

Успешное усвоение материала предполагает знание студентами основных положений курсов «Информатика» и «Организация ЭВМ и вычислительных систем».

Дисциплина является предшествующей для изучения дисциплин: «Основы информационной безопасности», «Безопасность систем баз данных» «Криптографические методы защиты информации», и др.

### **Требования к результатам освоения дисциплины:**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

**ОПК-8** – способностью к освоению новых образцов программных, технических средств и информационных технологий

**ПСК-7.4** – способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах

### **В результате изучения дисциплины студенты должны:**

#### **знать:**

- принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; основные модели данных, физическую организацию баз данных;
- последовательность и содержание этапов проектирования баз данных;
- средства обеспечения безопасности данных; основные понятия баз данных;
- примеры реализаций современных систем управления базами данных;
- современные подходы к организации и проведению научных исследований с использованием информационных технологий;
- основные термины по проблематике информационной безопасности; определение политики безопасности.

#### **уметь:**

- выделять сущности и связи предметной области; отображать предметную область на конкретную модель данных; создавать объекты базы данных;
- выполнять запросы к базе данных; создавать структуру взаимосвязанных объектов баз данных; воспользоваться основными предложениями языка SQL для составления запросов; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
- составлять основные виды запросов к БД с использованием языка SQL;
- составлять сложные виды запросов к БД с использованием языка SQL;
- применять современные технологии и методы программирования для создания интерфейсов прикладных программ к базам данных;
- оценивать эффективность и надежность защиты СУБД; средства обеспечения безопасности баз данных: контроля целостности информации.

#### **владеть навыками:**

- семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных;
- методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения; основными методологиями проектирования БД;
- современными методологиями проектирования БД навыками разработки документирования баз данных с учетом требований информационной безопасности

	<p><b>Основные разделы:</b></p> <p>Введение в базы данных. Модели и типы данных. Теоретико-графовые модели данных. Общие понятия реляционного подхода к организации БД. Проектирование реляционных БД. Инфологическое моделирование. Средства автоматизации проектирования. Язык SQL. Информационные системы в сетях. Распределенная обработка данных. Модели транзакций. Oracle Database . MySQL Server.</p> <p><b>Общая трудоемкость дисциплины 5 зачетных единицы (180 часов):</b></p> <p>аудиторные часы – 90 часов, самостоятельная работа – 90 часов, курсовая работа.</p> <p>Основные виды учебной работы: лекции; практические занятия; самостоятельная работа студентов. Форма проведения аттестации – зачет, зачет с оценкой и курсовая работа.</p>	
<p><b>Б1.В.ОД.3</b></p>	<p style="text-align: center;"><b>МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p>Цель изучения дисциплины: исследовать источники информационных угроз и стандарты информационной безопасности, методические документы ФСТЭК и ФСБ; выявлять источники и способы реализации угроз информационной безопасности, разрабатывать модели угроз с учетом различных факторов; исследовать и оценивать существующие модели.</p> <p>Изучение дисциплины базируется на знаниях, умениях и навыках, полученных в результате освоения <b>дисциплин</b> «Информатика», «Языки программирования», , «Технологии и методы программирования», «Теория графов».</p> <p>Знания и умения, полученные студентами при изучении дисциплин «Анализ рисков информационной безопасности», «Моделирование систем и процессов защиты информации»..</p> <p>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</p> <ul style="list-style-type: none"> <li>– <b>ОПК-3</b> способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</li> <li>– <b>ПК-4</b> способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</li> </ul> <p>В результате изучения дисциплины обучающийся должен:</p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>– физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем</li> <li>– Способы реализации угроз безопасности информации и модели нарушителя в автоматизированных системах</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>– анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности</li> <li>– разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем</li> </ul> <p><b>владеть/ владеть навыками:</b></p> <ul style="list-style-type: none"> <li>– навыками применения аппарата моделирования для решения прикладных теоретико-информационных задач</li> <li>– методами мониторинга и аудита, выявления угроз информационной</li> </ul>	<p><b>180(5)</b></p>



	<p>безопасности автоматизированных систем – методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения</p> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Цели и задачи моделирования угроз ИБ. Этапы моделирования угроз ИБ. Описание используемых технических средств и их назначение. Схема подключения технических средств. Архитектура информационной системы.</p> <p>Определение источников угроз. Выявление критических объектов информационной системы.</p> <p>Определение перечня угроз для каждого критического объекта. Выявление способов реализации угроз.</p> <p>Оценка материального ущерба и других последствий возможной реализации угроз, ранжирование угроз по потенциальному ущербу</p> <p>Разработка модели информационной безопасности с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании.</p> <p>Составление модели нарушителя, типы нарушителей, категории нарушителей</p> <p>Описания видов нарушителей и их возможностей (внутренние, внешние); описание каналов доступа в ИС (физические, общедоступные, технические)</p> <p>Описание данных видов нарушителей с привязкой к штатной структуре организации; описание возможностей данных нарушителей; определение актуальности каждого из видов нарушителей..</p>	
<p><b>Б1.В.ОД.4</b></p>	<p style="text-align: center;"><b>АЛГОРИТМЫ ШИФРОВАНИЯ ИНФОРМАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины «Алгоритмы шифрования информации» является формирование у студентов понятий об основных методах шифрования, криптографических протоколах, базовых алгоритмах, применяемых в криптосистемах, алгоритмах шифрования с симметричным и несимметричным ключом. Овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВПО для специальности 10.05.03 Информационная безопасность автоматизированных систем.</p> <p><b>Место дисциплины в структуре ООП:</b> Для усвоения данной дисциплины студенту необходим объем знаний, предусмотренный курсами информатики, дискретной математики, организации ЭВМ и вычислительных систем, технологии и методы программирования, языки программирования.</p> <p>Данная дисциплина необходима для последующего успешного выполнения научно-исследовательской работы.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-9.</b> Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>ПК-10.</b> Способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>В результате изучения дисциплины студент должен:</b> <b>знать:</b> Способы программно-аппаратной реализации наиболее устойчивых алгоритмов шифрования Основные протоколы обмена информацией между элементами автоматизированной системы</p>	<p><b>180 (5)</b></p>

	<p>Алгоритмы шифрования применяемые при обмене информации в автоматизированной системе</p> <p>Основы электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных</p> <p>Возможные комбинации программно-аппаратных компонентов для построения наиболее эффективного использования их ресурсов при построении узлов автоматизированной системы</p> <p><b>уметь:</b>  Реализовывать защищенный обмен информацией в автоматизированной системе  Реализовывать программно-аппаратные компоненты защищенных автоматизированных систем</p> <p><b>владеть навыками:</b>  Способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности</p> <p><b>Дисциплина включает в себя следующие разделы:</b>  Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шрифты. Шифрование с открытым ключом. Хеш-функции. Криптографические протоколы, протоколы обмена ключами. Основы криптоанализа.</p>	
<p><b>Б1.В.ОД.5</b></p>	<p align="center"><b>МЕТОДЫ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, АТТЕСТАЦИЯ АИС</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Целью дисциплины «Методы выявления нарушений информационной безопасности, аттестация АИС» является формирование профессиональных навыков аттестационных испытаний ОИ, изучение методик проведения аттестации, овладение методами мониторинга и аудита АС и подготовка к деятельности, связанной с аттестацией АИС в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Методы выявления нарушений информационной безопасности, аттестация АИС» рассматривает базовые теоретические понятия, средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Методы выявления нарушений информационной безопасности, аттестация АИС» входит в цикл дисциплин Б1.В.ОД.5 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем. Успешное усвоение материала предполагает знание студентами основных положений курсов «Введение в специальность», «Основы информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Техническая защита информации», «Безопасность сетей ЭВМ».</p> <p>Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем», «Моделирование угроз информационной безопасности», «Информационная безопасность распределенных информационных систем».</p> <p><b>Изучение дисциплины направлено на формирование и развитие</b></p>	<p><b>180 (5)</b></p>

	<p><b>следующих компетенций:</b></p> <p><b>ПК-16</b> - способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации.</p> <p><b>ПК-22</b> - способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации.</p> <p><b>ПСК-7.3</b> - способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем.</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</li> <li>- Организацию защиты информации на объектах информатизации.</li> <li>- Средства организации аттестации ВП по требованиям безопасности информации.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- Самостоятельно проводить мониторинг угроз безопасности автоматизированных систем.</li> <li>- Самостоятельно организовывать защиту информации на объектах информатизации и контролировать эффективность ее реализации.</li> <li>- Проводить научно-исследовательские работы при аттестации системы защиты информации с учетом требований к обеспечению информационной безопасности.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- Методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.</li> <li>- Методами и средствами защиты информации.</li> <li>- Навыками проведения аудита уровня защищенности и аттестацию информационных систем в соответствии с существующими нормами.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Общие положения проведения аттестационных испытаний. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте. Методики проведения аттестации. Методика аттестационных испытаний выделенных помещений по требованиям безопасности информации.</p>	
<p><b>Б1.В.ОД.6</b></p>	<p align="center"><b>АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p><b>Цель изучения дисциплины:</b>  формирование у студентов понятий об организации и методологии обеспечения информационной безопасности в государственных и коммерческих организациях на основе российских и международных стандартов, о процессе управления информационной безопасностью и его составляющих, об особенностях системы управления информационной безопасностью организации, об этапах планирования, реализации, проверки и совершенствования систем управления информационной безопасностью.</p> <p>Изучение дисциплины базируется на знаниях, умениях и навыках, полученных в результате освоения <b>дисциплины</b> «Безопасность сетей ЭВМ», «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем».</p> <p>Знания и умения, полученные студентами при изучении дисциплины, <b>необходимы при</b> выполнении научно-исследовательской работы.</p>	<p><b>144(4)</b></p>

Изучение дисциплины направлено на формирование и развитие следующих компетенций:

**ПК-5** – способность проводить анализ рисков информационной безопасности автоматизированной системы

**ПСК-7.2.** – способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах

**В результате изучения дисциплины обучающийся должен:**

**знать:**

- способы применения анализа рисков в информационной безопасности при работе над инновационными проектами перечень информационно-технологических ресурсов, подлежащих защите
- методы и процедуры выявления угроз информационной безопасности в защищённых распределённых приложениях; Способы обеспечения информационной безопасности систем организационного управления

**уметь:**

- применять базовые постулаты анализа рисков информационной безопасности при работе над междисциплинарными и инновационными проектами; выполнять анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
- выполнять анализ рисков информационной безопасности в распределенных информационных системах; использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы

**владеть навыками:**

- навыками применения анализа рисков информационной безопасности при работе над инновационными проектами; навыками анализа особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите
- методиками проведения анализа рисков информационной безопасности распределенных информационных систем; навыками семантического моделирования данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения.

**Дисциплина включает в себя следующие разделы:**

.Аспекты проблемы информационной безопасности

Оценочные стандарты в информационной безопасности.

Стандарты управления информационной безопасностью.

Содержание этапов разработки и внедрения системы управления ИБ.

Методика оценки рисков информационной безопасности предприятия.

Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей.

Методика оценки рисков информационной организации.

Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность.

Методики и технологии управления рисками.

Качественные методики управления рисками. Количественные методики управления рисками.

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.

9 Современные методы и средства анализа и управление рисками информационных систем.

**Цель дисциплины:** Целью освоения дисциплины «Моделирование систем и процессов защиты информации» является формирование у студентов знаний по основам организации, управления и обеспечения безопасности и целостности данных информационных систем и технологий, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах, ознакомление с принципами моделирования систем технического зрения, реализующих новые информационные оптические технологии; – изучение инструментальных (программных и технических) средств моделирования процессов функционирования оптоинформационных систем; – реализация моделирующих алгоритмов для исследования характеристик и поведения систем технического зрения; освоение принципов имитационного моделирования и математической формализации физических процессов, происходящих при работе оптико-электронных систем технического зрения.

**Место дисциплины в структуре ООП:** Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Информатика», «Основы информационной безопасности», «Информационные технологии. Базы данных», «Безопасность сетей ЭВМ» «Безопасность систем баз данных», «Безопасность операционных систем», «Анализ рисков информационной безопасности».

**Требования к результатам освоения дисциплины:** процесс изучения «Моделирование систем и процессов защиты информации» направлен на формирование следующих компетенций:

**ПК-2** – способностью разрабатывать и исследовать модели автоматизированных систем

**ПСК 7.1** – способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах

**В результате изучения дисциплины студенты должны:**

**знать:**

- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности.

**уметь:**

- разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем.

**владеть навыками:**

- методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем

**Основные дидактические единицы (разделы).** Этапы проектирования СИБ и требования к ним. Типовая структура комплексной системы защиты информации от несанкционированного доступа (НСД); Классы каналов НСД АС и средств вычислительной техники. Особенности многопользовательских систем. Типовые элементы структуры СИБ, включающей организационные и программно-технические решения по защите информации от НСД. Мониторинг и контроль состояния окружающей среды; ведение специальной информационной базы данных СИБ. Использование объединенной базы данных параметров окружающей среды для формирования особых функций

	<p>защиты с элементами прогнозирования. Методы и методики проектирования: методика выявления возможных каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, моделирование как инструментарий проектирования, методика построения административного управления КСИБ. Целевая функция задач защиты информации. Критерии достижения требуемого уровня. Последовательность работ и особенности при проектировании системы защиты информации от НСД. Утечка информации за счет ПЭМИН. Типовые решения защиты от ПЭМИН. Моделирование процессов утечки информации, модели нарушителя, основные критерии, типовые этапы моделирования. Методы и методики оценки качества СИБ: методы нормативного функционального наблюдения. Метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера, требования к эксплуатационной документации СИБ. Аттестация по требованиям безопасности; особенности эксплуатации</p> <p>Требования к эксплуатационной документации СИБ. Аттестация по требованиям безопасности; особенности эксплуатации СИБ на объекте защиты, организационно-функциональные задачи службы безопасности. Состав и содержание эксплуатационной документации. Проведение аттестационных испытаний СИБ. Нормативно-правовая документация по использованию СИБ. Организационные вопросы обеспечения СИБ. Допуск на объект. Служба безопасности: основные положения, регламентные документы, подбор кадров.</p>	
<p><b>Б1.В.ОД.8</b></p>	<p style="text-align: center;"><b>ПРОДВИЖЕНИЕ НАУЧНОЙ ПРОДУКЦИИ</b></p> <p><b>1 Цели освоения дисциплины</b></p> <p>Целями освоения дисциплины «Продвижение научной продукции» являются:</p> <ul style="list-style-type: none"> <li>- развитие у студентов личностных качеств, а также формирование профессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем;</li> <li>- 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;</li> <li>- освоение студентами навыков проведения патентного поиска, оформления патентной документации</li> </ul> <p><b>2 Место дисциплины в структуре образовательной программы подготовки бакалавра</b></p> <p>Дисциплина «Продвижение научной продукции» входит в вариативную часть блока 1 образовательной программы.</p> <p>Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения истории, правоведения, экономики.</p> <p>Знания и умения студентов, полученные при изучении дисциплины «Продвижение научной продукции» будут необходимы им при дальнейшей подготовке к ГИА</p> <p><b>3 Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения</b></p> <p><b>ОПК-5</b> способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> <p><b>ОК-8:</b> способностью к самоорганизации и самообразованию</p>	

	<p><b>В результате изучения дисциплины студенты должны:</b></p> <p><b>знать:</b> основные понятия и определения федерального закона «О науке и государственной научно-технической политике»; основные понятия и определения федерального закона об инновационной деятельности и о государственной инновационной политике; систему финансирования инновационной деятельности. Порядок и особенности выполнения научно- исследовательских работ по государственным контрактам; формы государственной поддержки инновационной деятельности в России. Принципы, формы и методы финансирования научно-технической продукции</p> <p><b>уметь:</b> приобретать знания в области продвижения научной продукции; выделять особенности продвижения товара и пути его совершенствования в условиях Российского рынка научной продукции; определять эффективные пути продвижения научной продукции с применением современных информационно-коммуникационных технологий, глобальный информационный4 основные шаги и правила государственной системы регистрации результатов научной деятельности</p> <p><b>владеть навыками:</b> классификацией научно-технической продукции, профессиональным языком предметной области знания; практическими навыками оценки качества для научно-технической продукции, навыками составления конкурсной документации; методами стимулирования сбыта продукции, способами оценивания значимости и практической пригодности инновационной продукции; способами анализа патентной документации и проведения патентного поиска</p> <p><b>Основные дидактические единицы (разделы).</b> Понятие научной продукции Виды научной продукции Регистрация различных видов научной продукции Пути продвижения на рынок Системы финансирования Системы государственной поддержки Принципы взаимодействия с промышленными предприятиями Конкурсная документация и ее оформление.</p>	
Б1.В.ДВ	<b>ДИСЦИПЛИНЫ ПО ВЫБОРУ</b>	
	<b>ЭЛЕКТИВНЫЕ КУРСЫ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ</b>	
Б1.В.ДВ.1		
1	<p style="text-align: center;"><b>ОСНОВЫ РАДИОТЕХНИКИ</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины «Основы радиотехники» являются: обучение методам и основам построения информационных систем и устройств формирования, передачи, приема и обработки сигналов, радиотехнических способов защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b> Дисциплина «Основы радиотехники» входит в математический и</p>	180 (5)

	<p>естественнонаучный цикл образовательной программы по подготовки специальности 090303 «Информационная безопасность автоматизированных систем по специализации обеспечение информационной безопасности распределенных информационных систем».</p> <p>Для изучения дисциплины необходимы знания, умения, навыки, сформированные в результате изучения дисциплин:</p> <ol style="list-style-type: none"> <li>1. «Физика» (разделы: электричество, магнетизм).</li> <li>2. «Математический анализ» (разделы: дифференциальные и интегральные исчисления, функции комплексных переменных, методы решения дифференциальных уравнений, решение задач комплексным методом).</li> <li>3. Иностранный язык (преимущественно – английский язык)</li> <li>4. Информатика (в полном объеме)</li> </ol> <p>Знания, умения, навыки, полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: «программно-аппаратные средства обеспечения информационной безопасности», «разработка и эксплуатация защищенных автоматизированных систем», «методы выявления нарушений информационной безопасности», «аттестация АИС».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-10</b> 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 профессиона</p> <p><b>ОПК-1</b> способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- физическую сущность процессов, происходящих в системах передачи информации в целом</li> <li>- программное обеспечение для анализа систем передачи информации в целом;</li> <li>- аппаратуру и программное обеспечение для проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- разрабатывать модели процессов, происходящих в системах передачи информации в целом</li> <li>- проводить анализ систем передачи информации в целом;</li> <li>- использовать аппаратуру и программное обеспечение для проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом</li> <li>- методами исследования систем передачи информации в целом;</li> <li>- методами проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b>  Основа построения радиотехнических устройств приема и передачи информации. Преобразование информационных сигналов в радиотехнических системах и коммуникационных сетях. Радиотехнические способы защиты информации.</p>	
2	<p align="center"><b>ФИЗИЧЕСКИЕ ОСНОВЫ ПЕРЕДАЧИ ИНФОРМАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b></p>	180 (5)



	<p>Целями освоения дисциплины «Физические основы передачи информации» являются: обучение методам и основам построения информационных систем и устройств формирования, передачи, приема и обработки сигналов, радиотехнических способов защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Основы радиотехники» входит в математический и естественнонаучный цикл образовательной программы по подготовки специальности 090303 «Информационная безопасность автоматизированных систем по специализации обеспечение информационной безопасности распределенных информационных систем».</p> <p>Для изучения дисциплины необходимы знания, умения, навыки, сформированные в результате изучения дисциплин:</p> <ol style="list-style-type: none"> <li>1. «Физика» (разделы: электричество, магнетизм).</li> <li>2. «Математический анализ» (разделы: дифференциальные и интегральные исчисления, функции комплексных переменных, методы решения дифференциальных уравнений, решение задач комплексным методом).</li> <li>3. Иностранный язык (преимущественно – английский язык)</li> <li>4. Информатика (в полном объеме)</li> </ol> <p>Знания, умения, навыки, полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: «программно-аппаратные средства обеспечения информационной безопасности», «разработка и эксплуатация защищенных автоматизированных систем», «методы выявления нарушений информационной безопасности», «аттестация АИС».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-10</b> 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 профессиона</p> <p><b>ОПК-1</b> способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- физическую сущность процессов, происходящих в системах передачи информации в целом</li> <li>- программное обеспечение для анализа систем передачи информации в целом</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- разрабатывать модели процессов, происходящих в системах передачи информации в целом</li> <li>- проводить анализ систем передачи информации в целом</li> </ul> <p><b>владеть:</b></p> <ul style="list-style-type: none"> <li>- математическим аппаратом для описания процессов, происходящих в системах передачи информации в целом</li> <li>- методами исследования систем передачи информации в целом</li> </ul> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Основы построения радиотехнических устройств приема и передачи информации. Преобразование информационных сигналов в радиотехнических системах и коммуникационных сетях. Радиотехнические способы защиты информации.</p>	
Б1.В.ДВ.2		
1	<p style="text-align: center;"><b>ОСНОВЫ ТЕОРИИ ОПТИМИЗАЦИИ</b></p> <p><b>Цели изучения дисциплины:</b></p>	144 (4)

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».

**Место дисциплины в структуре ООП:**

Дисциплина «Основы теории оптимизации» входит в цикл дисциплин Б1.В.ДВ.2.1 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем и является дисциплиной по выбору.

Для освоения дисциплины студенты используют знания, умения и компетенции, сформированные в ходе изучения основных положений курсов «Алгебра и Геометрия», «Математический анализ», «Математическая логика и теория алгоритмов» и «Теория вероятностей, математическая статистика».

Дисциплина является предшествующей для изучения дисциплин: «Моделирование угроз информационной безопасности», «Моделирование систем и процессов защиты информации».

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**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.

**ПК-2** - способностью создавать и исследовать модели автоматизированных систем.

**ПСК-7.1** - способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.

**В результате изучения дисциплины студент должен:**

**знать:**

- Основные понятия математического анализа, дифференциальной геометрии, численные методы.
- Основные методы и технологии проектирования, моделирования, исследования автоматизированных систем.
- Способы применения теоретических положений и методов теории оптимизации для постановки и решения профессиональных задач.

**уметь:**

- Разрабатывать алгоритмы численного решения задач оптимизации.
- Находить оптимальные стратегии.
- Эффективно использовать и оптимизировать свою работу за счет применения общих положений и методов теории оптимизации.

**владеть:**

- Навыками повышения эффективности работы за счет применения общих положений и методов теории оптимизации.
- Навыками использования стандартных методов и моделей математического анализа, теории оптимизации, а так же их применения к решению прикладных задач.
- Навыками реализации задач оптимизации посредством программного обеспечения общего назначения и методо-ориентированного программного обеспечения.

	<p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Предмет и содержание дисциплины. Линейное программирование. Методы решения ЗЛП. Применение общей задачи линейного программирования для решения прикладных задач. Решение задач комбинаторной оптимизации. Моделирование систем. Решение задач одномерной оптимизации. Моделирование систем. Решение задач многомерной оптимизации. Решение прикладных задач методами оптимизации.</p>	
<p>2</p>	<p><b>МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ</b></p> <p><b>1. Цели освоения дисциплины</b></p> <p>Целями изучения дисциплины «Математическое моделирование распределенных систем» являются: освоение моделей управления, получение знаний о закономерностях и свойствах процессов управления распределенными объектами, систематическое изучение основ теории и практики математического и имитационного моделирования систем; изучение основных подходов и математических схем к построению имитационных моделей; изучение возможностей применения имитационных моделей; освоение методологий и актуальных CASE-средств для имитационного моделирования систем и процессов и формирования у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО для специальности «Информационная безопасность автоматизированных систем».</p> <p><b>2. Место дисциплины в структуре образовательной программы подготовки специалиста</b></p> <p>Дисциплина «Математическое моделирование распределенных систем» входит вариативную часть образовательной программы по специальности 100503 «Информационная безопасность автоматизированных систем».</p> <p>Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплины «Математический анализ».</p> <p>Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплины «Моделирование систем и процессов защиты информации».</p> <p><b>3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения</b></p> <p>В результате освоения дисциплины (модуля) обучающийся должен обладать следующими компетенциями:</p> <p><b>ОПК-2</b> способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов</p> <p><b>ПК-2</b> способностью создавать и исследовать модели автоматизированных систем</p> <p><b>ПСК-7.1</b> способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студенты должны:</b></p> <p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;</li> <li>- основные принципы и схемы автоматического управления; Основные</li> </ul>	<p><b>144 (4)</b></p>

	<p>требования нормативно-правовой базы в области защиты информации</p> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;</li> <li>применять методы расчета и исследования систем автоматического управления объектами с распределенными параметрами</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности распределенных систем</li> </ul> <p><b>Основные дидактические единицы (разделы).</b> Моделирование динамических характеристик систем с сосредоточенными параметрами. Особенности построения математических моделей. Подходы к построению моделей сложных систем. Имитационное моделирование случайных процессов в измерительных приборах и системах. Математические модели в интегральной форме. Решение краевых задач методами конечно - разностной аппроксимации по координатам в системах математического моделирования для персональных компьютеров. Условия устойчивости решений. Особенности моделирования физических полей в неоднородных и анизотропных средах.</p>	
<b>Б1.В.ДВ.3</b>		
1	<p align="center"><b>ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА</b></p> <p><b>Цель дисциплины:</b> 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, а также содействие фундаментализации образования и развитию системного мышления.</p> <p><b>Место дисциплины в структуре ООП:</b> Дисциплина «Защита электронного документооборота» входит в вариативную часть образовательной программы по специальности 100503 Информационная безопасность автоматизированных систем.</p> <p>Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Математический анализ», «Дискретная математика», «Информатика», «Организация ЭВМ и вычислительных систем» «Языки программирования», «Теория вероятностей, математическая статистика», «Технологии и методы программирования». Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Теория графов и ее приложения», «Информационные технологии. Базы данных», «Анализ рисков информационной безопасности».</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения «Защита электронного документооборота» направлен на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы</li> <li>ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</li> <li>ПК-28 способностью управлять информационной безопасностью автоматизированной системы</li> </ul> <p><b>В результате изучения дисциплины студенты должны:</b></p>	144 (4)

	<p><b>Знать:</b> - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);</p> <p><b>уметь:</b> - разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;</p> <p><b>владеть навыками:</b> - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;</p> <p><b>Основные разделы:</b> Функции, задачи и особенности электронного документооборота. Этапы проектирования и классы системы электронного документооборота. Проектирование и внедрение защищенного электронного документооборота. Организационные и правовые основы использования ЭЦП. ФЗ №1 «Об электронной цифровой подписи». Обзор основных алгоритмов ЭЦП. Проблемы аутентификации пользователей и ЭЦП в информационных структурах. Классификация угроз систем документооборота. Угрозы конфиденциальности. Угрозы работоспособности системы. Обеспечение сохранности документов, обеспечение безопасного доступа, обеспечение подлинности документов, протоколирование действия пользователей. Идентификация, аутентификация, авторизация пользователей, разграничение прав доступа. . Системы предотвращения утечек информации. Обзор и сравнение российских и зарубежных dlp-систем. Криптографическая защита, применение электронных подписей, цифровое уничтожение.</p>	
<p><b>Б1.В.ДВ.3</b> <b>2</b></p>	<p align="center"><b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ</b></p> <p><b>Цель дисциплины:</b> Целью освоения дисциплины является формирование у студентов знаний по основам организации, управления и обеспечения безопасности и целостности данных информационных систем и технологий, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах.</p> <p><b>Место дисциплины в структуре ООП:</b> Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин «Информатика», «Основы информационной безопасности», «Информационные технологии. Базы данных», «Безопасность сетей ЭВМ» «Безопасность систем баз данных», «Безопасность операционных систем», «Моделирование угроз информационной безопасности», «Анализ рисков информационной безопасности».</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения «Информационная безопасность систем организационного управления» направлен на формирование следующих компетенций:  <b>ПК-13</b> способностью участвовать в проектировании средств защиты информации автоматизированной системы  <b>ПК-24</b> способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности  <b>ПК-28</b> способностью управлять информационной безопасностью автоматизированной системы</p> <p><b>В результате изучения дисциплины студенты должны:</b>  <b>знать:</b>  - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;  - организацию защиты информации от утечки по техническим каналам на объектах информатизации;  - программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами</p>	<p><b>144 (4)</b></p>

	<p>данных, компьютерных сетях;</p> <ul style="list-style-type: none"> <li>- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;</li> <li>- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;</li> <li>- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;</li> </ul> <p><b>Основные разделы:</b> Общая характеристика систем организационного управления. Понятие систем организационного управления. Автоматизированные системы организационного управления. Централизованная и децентрализованная система организационного управления. Классификация организационных информационных систем. Системы уровня знаний. Системы эксплуатационного уровня. Системы уровня управления. Системы стратегического уровня. Методология построения систем организационного управления. Угрозы информационной безопасности систем организационного управления. Методы и средства по обеспечению информационной безопасности систем организационного управления. Безопасность на уровне приложений. .Безопасность на уровне баз данных.Безопасность на уровне сетевых коммуникаций.</p> <p><b>Общая трудоемкость дисциплины</b> Общая трудоемкость дисциплины составляет <b>4 зачетных единицы 144 часа:</b> аудиторные часы – 72 часа, самостоятельная работа – 72 часа. Основные виды учебной работы: лекции; практические занятия; СРС. Форма проведения аттестации – экзамен.</p>	
<p><b>Б1.В.ДВ.4</b></p>		
<p><b>1</b></p>	<p style="text-align: center;"><b>ВИРТУАЛЬНЫЕ СЕТИ</b></p> <p><b>Цель дисциплины:</b> изучение архитектуры и настроек виртуальных локальных сетей (VLAN), виртуальных частных сети (VPN) и технологий на их основе Site-to-site VPN, FlexVPN и SSL VPN, освоение облачных технологий виртуальных сетей.</p> <p><b>Место дисциплины в структуре ООП:</b> Дисциплина «Виртуальные сети» относится к вариативной части профессионального цикла дисциплин по специальности «Информационная безопасность автоматизированных систем». Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Сети и системы передачи информации».</p> <p><b>Требования к результатам освоения дисциплины:</b> процесс изучения дисциплины «Виртуальные сети» направлен на формирование следующих компетенций:</p> <p><b>ПК-10.</b> 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 профессиона</p> <p><b>ПК-24</b> способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p>	<p>180 (5)</p>

**ПСК-7.4** способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах

**В процессе изучения дисциплины студенты должны:**

**Знать:**

- К Типовые структуры и принципы организации компьютерных сетей.
- К Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей.
- К Основные протоколы компьютерных сетей.
- К Последовательность и содержание этапов построения компьютерных сетей.
- К Принципы построения и функционирования систем и сетей передачи информации.
- К Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях.

**Уметь:**

- К Проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети.
- К Эффективно использовать различные методы и средства защиты информации для компьютерных сетей.
- К Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.

**Владеть:**

- К Навыками обеспечения безопасности информации с помощью стандартных сетевых средств обмена информацией.
- К Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита), локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности.
- К Навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности.
- К Навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей.

**Основные (разделы):**

**Виртуальные локальные сети (VLAN):** сегментация и типы VLAN, голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet. Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Динамический протокол инициализации транка (DTP). Поиск неисправностей при использовании VLAN. Рекомендации по дизайну VLAN. Организация маршрутизации между VLAN. Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.

**Виртуальные частные сети (VPN).** Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Типы VPN: Site-to-Site VPN (LAN-to-LAN VPN) и Remote access VPN. Основные компоненты для каждой VPN-технологии. Протоколы работы VPN: протокол GRE, конфигурирование простого Site-to-Site туннельного соединения; протокол PPTP, конфигурирование клиент-серверного соединения с использованием PPTP на маршрутизаторе и рабочей станции; протокол L2TP, конфигурирование клиент-серверного соединения с использованием L2TP на маршрутизаторе и рабочей станции; протокол PPPoE, конфигурирование соединения с использованием PPPoE на маршрутизаторах. Протокол ISAKMP, фазы построения туннеля. Технология IPSec, криптографические алгоритмы: алгоритмы шифрования, алгоритмы хеширования, алгоритмы безопасного обмена ключами. Dynamic VPN, конфигурирование функций динамического VPN-концентратора на маршрутизаторе. Remote Access IPSec VPN.

**Технологии Site-to-site VPN, FlexVPN и SSL VPN.** Конфигурирование

	<p>классического туннельного соединения для объединения офисных сетей. Топологии и технологии для S2S VPN. IPsec VPN. Работа IKE и IKEv2. Протокол ESP. Виртуальные интерфейсы VPN (VTI). Работа DMVPN. Настройка Point-to-Point (P2P) VPN на Cisco ASA. Реализация Site-to-site IPsec VPN с использованием SDM. Основные преимущества и возможности технологии FlexVPN. Использование Cisco IOS FlexVPN. Работа P2P FlexVPN. Типовые сценарии FlexVPN. Работа Point-to-Multipoint (Hub-and-Spoke) IPsec VPN, используя FlexVPN. Централизованное конфигурирование узлов-участников. Преимущества SSL VPN. SSL и TLS. Установка соединения. Подтверждение подлинности как сервера, так и клиента. Групповые политики SSL-клиентов на Cisco ASA и connection profiles. Настройка SSL VPN на Cisco ASA. Настройка и использование Cisco AnyConnect VPN. Настройка отдельных компонентов - аутентификации клиента и сервера, назначения IP-адресов, работы split tunneling, групповых политик и Identity NAT. Параллельные туннели для TLS и DTLS. Управление ПО клиента со стороны Cisco ASA. Работа с Trusted Network Detection и настройка AnyConnect SBL (Start Before Logon). Аутентификация на базе x.509-сертификатов. Отзыв сертификатов и проверка на отзыв у клиентов. Многофакторная аутентификация и авторизация с Cisco ISE. Настройка AnyConnect IPsec с IKEv2.</p> <p><b>Облачные технологии виртуальных сетей.</b> Характеристики аппаратно-программных платформ виртуализации (VMware vSphere, Microsoft HyperV, Citrix XenServer, RedHat RHEV) для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS (Amazon Web Services Elastic Compute Cloud, Cisco Systems CloudVerse, Google Compute Engine, Microsoft Azure и др.). Отличия технологий построения виртуальных сетей в физической сетевой среде и в облачной (виртуальной) сетевой среде. Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами. 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). Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA). Сетевая архитектура облака, развитие технологии Ethernet в облачной среде передачи данных Data Center Bridging (DCB), расширенный протокол xSTP (Spanning Tree Protocol, технология VEB (Virtual Ethernet Bridge), метод передачи трафика сети хранения данных Fibre Channel по сети Ethernet FCoE (Fibre Channel over Ethernet), технология расширения концепции использования Fabric Extender до уровня виртуальных машин VM-FEX (Virtual Machine Fabric Extender), распределенные виртуальные коммутаторы, интегрированные со средой виртуализации Cisco Nexus 1000V. Создание VPN-серверов для виртуальных частных сетей в облаке.</p> <p><b>Общая трудоемкость дисциплины.</b> Общая трудоемкость дисциплины составляет <b>5</b> зачетных единиц (<b>180</b> часов): аудиторная работа – 108 часов (лекции – 54 часа, практические занятия – 54 часа), самостоятельная работа – 72 часа. Основные виды учебной работы: лекции; практические занятия; самостоятельная работа студентов. Форма проведения аттестации – зачет с оценкой.</p>	
2	<p style="text-align: center;"><b>ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</b></p> <p><b>Цель дисциплины:</b> Освоить технические, правовые и организационные средства защиты от несанкционированного использования и копирования программного обеспечения. Изучить методы противодействия разрушению, нарушения целостности и достоверности программного обеспечения.</p> <p><b>Место дисциплины в структуре ООП:</b> Дисциплина «Защита программного обеспечения» относится к вариативной части профессионального цикла дисциплин по специальности «Информационная</p>	180 (5)



безопасность автоматизированных систем». Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Дискретная математика», «Математическая логика и теория алгоритмов», «Теория информации», «Языки программирования», «Криптографические методы защиты информации», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Алгоритмы шифрования информации», «Моделирование систем и процессов защиты информации», «Безопасность операционных систем».

**Требования к результатам освоения дисциплины:** процесс изучения дисциплины «Защита программного обеспечения» направлен на формирование следующих компетенций:

**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 профессиона

**ПК-24** способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

**ПСК-7.4** способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах

**В результате изучения дисциплины студенты должны:**

**Знать:**

- К Состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.
- К Методы проведения расследования компьютерных инцидентов.
- К Способы обнаружения и нейтрализации последствий вторжений в компьютерные системы.
- К Основные принципы построения систем обнаружения компьютерных атак.
- К Методы и методики оценивания безопасности компьютерных систем.
- К Назначение и алгоритм работы программных продуктов, типы поддерживаемых аппаратных платформ.

**Уметь:**

- К Применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска).
- К Анализировать программные компоненты автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности.
- К Проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
- К Выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.
- К Анализировать компьютерную систему с целью определения уровня защищенности и доверия.
- К Определять причины, цели и условия изменения свойств и состояния программного обеспечения.
- К Выявлять индивидуальные признаки программы, позволяющие впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы.

	<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>К Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) программных систем с учетом требований по обеспечению информационной безопасности.</li> <li>К Разработкой предложений по устранению выявленных уязвимостей.</li> <li>К Определением уровня защищенности и доверия при проведении анализа компьютерной системы.</li> <li>К Средствами автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем.</li> <li>К Навыками программирования с использованием эффективных реализаций структур данных и алгоритмов.</li> <li>К Выявлением, исследованием функциональных свойств и состояния программного обеспечения.</li> </ul> <p><b>Основные разделы дисциплины:</b> Защита от несанкционированного использования и копирования. Классификация методов защиты по способу распространения защищаемого программного обеспечения и типу носителя лицензии. Технические средства защиты: локальная программная защита серийными номерами; сетевая программная защита для локальных и глобальных сетей; защита при помощи компакт-дисков, токенов и электронных ключей; привязка к параметрам компьютера и активация; защита программ от копирования путём переноса их в облачный сервис; защита обфускаторами кода программы от анализа; средства защиты программного обеспечения на мобильных платформах; недостатки и неудобства использования защищенных программ. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации. Методы и средства защиты программ от компьютерных вирусов. Методы и средства обеспечения целостности и достоверности используемого программного кода. Правовая и организационная поддержка процессов разработки и применения программного обеспечения. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Юридические средства защиты посредством лицензий и патентов на программное обеспечение. Организационные средства защиты. Сертификационные испытания программных средств. Уязвимости современных методов защиты программного обеспечения. Использование автоматических средств защиты программ.</p> <p><b>Общая трудоемкость дисциплины.</b> Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов): аудиторная работа – 108 часов (лекции – 54 часа, практические занятия – 54 часа), самостоятельная работа – 72 часа. Основные виды учебной работы: лекции; практические занятия</p>	
<b>Б1.В.ДВ.5</b>		
<b>Б1.В.ДВ.5.1</b>	<p align="center"><b>МЕТОДЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Общей целью дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВПО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Специальными целями дисциплины «Методы мониторинга информационной безопасности автоматизированных систем» являются: изучить архитектуру, функции, методы и алгоритмы, организационную структуру, технологии создания и готовые аппаратно-программные решения систем мониторинга информационной безопасности автоматизированных</p>	<b>216(6)</b>

систем;  
научится применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем.

**Место дисциплины в структуре ООП:**

Дисциплина «Методы мониторинга информационной безопасности автоматизированных систем» относится к вариативной части профессионального цикла дисциплин по специальности «Информационная безопасность автоматизированных систем». Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Моделирование систем и процессов защиты информации», «Безопасность операционных систем», «Методы выявления нарушений информационной безопасности, аттестация АИС», «Технология построения защищенных распределенных приложений», «Методы проектирования защищенных распределенных информационных систем», «Организационное и правовое обеспечение информационной безопасности», «Сети и системы передачи информации», «Техническая защита информации», «Основы информационной безопасности», «Безопасность сетей ЭВМ».

**Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

**ПК-15.** Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

**ПК-17.** Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

**ПК-24.** Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

**ПСК-7.3.** Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем.

**В результате изучения дисциплины студент должен:**

**знать:**

Особенности эксплуатации программно- аппаратных комплексов для проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

Эффективные способы выявления каналов утечки информации

Эффективные способы применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

Уязвимости распределенных систем, факторы приводящие к возникновению каналов утечки информации

**уметь:**

Использовать программно-аппаратных комплексов для проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

Выполнять инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

Эффективно применять информационно-технологические ресурсы автоматизированной системы при мониторинге информационной безопасности

Выполнять полный комплекс действий связанный с проведением аудита информационной безопасности распределённой системы

**владеть навыками:**

Навыками выполнения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

	<p>Практическими навыками определения каналов утечки информации при помощи средств мониторинга</p> <p>Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем</p> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Архитектура и функции систем мониторинга информационной безопасности. Организационная структура систем мониторинга информационной безопасности. Методы и алгоритмы выявления нарушений информационной безопасности в потоке сообщений автоматизированной системы. Исследование вероятностных характеристик нарушений информационной безопасности в потоке сообщений автоматизированной системы для выявления ошибок первого и второго рода. Аппаратно-программные решения обнаружения инцидентов информационной безопасности и управления ими, централизованного сбора информации по событиям из множества распределенных разнородных источников, обработки ее и анализа, контроля соответствия защищенности информационных систем корпоративным политикам и стандартам безопасности.</p>	
<p><b>Б1.В.ДВ.5.2</b></p>	<p align="center"><b>АНАЛИЗ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</b></p> <p><b>Цели изучения дисциплины:</b></p> <p>Общей целью дисциплины «Анализ безопасности 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 ВПО по специальности «Информационная безопасность автоматизированных систем».</p> <p>Специальными целями дисциплины «Анализ безопасности программного обеспечения» являются:</p> <p>изучить контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения и способы обеспечения надежности программ для контроля их технологической безопасности;</p> <p>освоить способы оценки эффективности систем защиты программного обеспечения и технологии разработки систем программно-технической защиты программного обеспечения</p> <p><b>Место дисциплины в структуре ООП:</b></p> <p>Дисциплина «Анализ безопасности программного обеспечения» относится к вариативной части профессионального цикла дисциплин по специальности «Информационная безопасность автоматизированных систем». Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Дискретная математика», «Математическая логика и теория алгоритмов», «Теория информации», «Языки программирования», «Криптографические методы защиты информации», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Алгоритмы шифрования информации», «Моделирование систем и процессов защиты информации», «Безопасность операционных систем».</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <p><b>ПК-15.</b> Способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем</p> <p><b>ПК-17.</b> Способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы</p>	<p align="center"><b>180 (5)</b></p>

	<p>утечки информации</p> <p><b>ПК-24.</b> Способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p><b>ПСК-7.4.</b> Способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p><b>В результате изучения дисциплины студент должен:</b></p> <p><b>знать:</b></p> <p>расширенные российские и базовые международные показатели качества программного обеспечения;</p> <p>методики комплексной проверки по и выявления каналов утечки информации</p> <p>способы эффективного использования информационно-технологических ресурсов для проведения анализа безопасности по</p> <p>особенности удалённого администрирования различных операционных систем</p> <p><b>уметь:</b></p> <p>проводить комплексное тестирование и отладку программных систем в полном объеме</p> <p>выполнять комплексный анализ по</p> <p>использовать гибридные методы оценки безопасности программного обеспечения</p> <p>управлять процессами, происходящими на удаленной рабочей станции или сервере баз данных</p> <p><b>владеть навыками:</b></p> <p>навыками исследования эффективности программных средств автоматизации в полном объеме;</p> <p>способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации</p> <p>статистическими методами анализа программного обеспечения</p> <p>способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах</p> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Теоретические и формальные методы (Флойда, Хоара, Маккарти, Дейкстры) доказательства правильности программ и их спецификаций. Контрольно-испытательные и логико-аналитические методы анализа безопасности программного обеспечения. Методы и средства анализа безопасности программ: лексический и синтаксический верификационный анализ, семантический анализ программ. Технологии создания алгоритмически безопасных процедур. Методы создания самотестирующихся и самокорректирующихся программ. Способы обеспечения надежности программ для контроля их технологической безопасности. Методы идентификации программ и их характеристик. Анализ средств и этапы преодоления систем защиты программного обеспечения. Технологии разработки систем программно-технической защиты программного обеспечения. Оценка эффективности систем защиты программного обеспечения.</p>	
ДВ*		
Б2	<b>ПРАКТИКИ</b>	
Б2.У	<b>УЧЕБНАЯ ПРАКТИКА</b>	
Б2.У.1	<b>УЧЕБНАЯ ПРАКТИКА ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ, В ТОМ ЧИСЛЕ</b>	<b>216(6)</b>

## **ПЕРВИЧНЫХ УМЕНИЙ И НАВЫКОВ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ**

### **Цели изучения дисциплины:**

Целями учебной практики по 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 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.

### **Место дисциплины в структуре ООП:**

Задачами учебной практики 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.

### **Изучение дисциплины направлено на формирование и развитие следующих компетенций:**

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач **(ОПК-1)**;
- способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности **(ОПК-3)**;
- способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах **(ОПК-4)**;
- способностью к освоению новых образцов программных, технических средств и информационных технологий **(ОПК-8)**;
- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке **(ПК-1)**.

### **В результате изучения дисциплины студент должен:**

#### **знать:**

- основные должностные инструкции инженера-программиста, сетевого администратора; специалиста в области информационных безопасности;
- краткую характеристику выпускаемой продукции, её технический уровень.
- взаимосвязь основных цехов и отделов предприятия и систему управления ими, своё место в этой системе;
- основные задачи, решаемые предприятием по совершенствованию информационной безопасности;
- действующие на предприятии правила внутреннего распорядка, техники безопасности, пожарной безопасности и режима работы предприятия;
- характеристики аппаратного и программного обеспечения локальной или корпоративной сети предприятия;
- принципы администрирования и обслуживания локальной или корпоративной сети предприятия;
- монтажа электронного оборудования и средств электронных коммуникаций.
- организационную структуру и функциональную часть автоматизированных систем управления (АСУ);
- политики безопасности и меры защиты в АС;
- комплексный подход к построению эшелонированной защиты для АС;
- принципы и стандарты построения современных автоматизированных

систем и подходы к интеграции сетей в автоматизированные системы;

- основные уязвимости и угрозы ИБ для автоматизированных систем;
- основные методы и средства реализации удаленных сетевых атак на автоматизированные системы;
- политики безопасности и меры защиты в автоматизированных системах;
- правовые основы и правила работы программно-аппаратных средств обеспечения ИБ АС;
- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; возможности и способы использования безопасных информационных технологий в работе современного предприятия при практической реализации требований отечественных и международных стандартов ИБ;
- условия создания и эксплуатации программно-аппаратных средств обеспечения ИБ АС;
- безопасные сетевые технологии, в которых используются программно-аппаратные средства обеспечения ИБ.

**уметь:**

- устанавливать операционную систему, устранять ее сбои, устанавливать необходимые драйверы и прикладные программы; выполнять резервирование системной информации;
- устанавливать платы расширения и подключать и конфигурировать различные периферийные устройства;
- администрировать рабочие станции и серверы;
- осуществлять поиск и защиты от компьютерных вирусов и программных закладок;
- работать с технической документацией;
- работать с измерительной и контролирующей техникой.
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенных систем;
- применять комплексный подход к обеспечению ИБ для АС;
- осуществлять управление и администрирование защищенных АС;
- анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным АС;
- определять и устранять основные угрозы ИБ для АС;
- строить модели угроз и нарушителя ИБ для АС и АС;
- выявлять и устранять уязвимости в основных компонентах АС;
- обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;
- проектировать защищенные АС; применять стандартные решения для защиты информации в АС и квалифицированно оценивать их качество;
- используя современные методы и средства, разрабатывать политику ИБ для АС;
- реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем;
- применять комплексный подход к обеспечению ИС для АС;
- осуществлять управление и администрирование защищенных АС;
- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе АС с целью обеспечения требуемого уровня ее защищенности;
- экономически эффективно использовать программно-аппаратные средства обеспечения ИБ информационных технологий в профессиональной деятельности;
- применять в различных проектах программно-аппаратные средства обеспечения ИБ.

**владеть навыками:**

- навыками анализа угроз ИБ и уязвимостей в АС;
- навыками распознавания сетевых атак на АС;
- навыками разработки политик ИБ для АС;

	-навыками использования программно-аппаратных средств обеспечения информационной безопасности АС.	
<b>Б2.Н</b>	<b>НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА</b>	
<b>Б2.Н.1</b>	<p align="center"><b>НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА</b></p> <p><b>Цели изучения дисциплины:</b>  Целями научно-исследовательской работы по 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 общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b>  В соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по специальности 10.05.03 «Информационная безопасность автоматизированных систем» ООП специалитета, научно-исследовательская работа относится к разделу «Практики». При выполнении научно-исследовательской работы студенты опираются на знания, умения и навыки, полученные в ходе предшествующего изучения дисциплин математического и естественнонаучного цикла, профессионального цикла. Усвоение знаний, полученных студентами на учебной практике, призвано повысить их профессионализм и компетентность, а также способствовать развитию у студентов творческого мышления, системного подхода к построению информационных технологий на предприятиях и в организациях.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <ul style="list-style-type: none"> <li>– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);</li> <li>– 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);</li> <li>– способностью создавать и исследовать модели автоматизированных систем (ПК-2);</li> <li>– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);</li> <li>– способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);</li> <li>– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);</li> <li>– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);</li> <li>– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя</li> </ul>	<b>540(15)</b>



информационной безопасности в распределенных информационных системах (ПСК-7.1);

**В результате изучения дисциплины студент должен:**

**знать:**

- основные должностные инструкции инженера-программиста, сетевого администратора; специалиста в области информационных безопасности;
- краткую характеристику выпускаемой продукции, её технический уровень.
- взаимосвязь основных цехов и отделов предприятия и систему управления ими, своё место в этой системе;
- основные задачи, решаемые предприятием по совершенствованию информационной безопасности;
- действующие на предприятии правила внутреннего распорядка, техники безопасности, пожарной безопасности и режима работы предприятия;
- характеристики аппаратного и программного обеспечения локальной или корпоративной сети предприятия;
- принципы администрирования и обслуживания локальной или корпоративной сети предприятия;
- монтажа электронного оборудования и средств электронных коммуникаций.
- организационную структуру и функциональную часть автоматизированных систем управления (АСУ);
- политики безопасности и меры защиты в АС;
- комплексный подход к построению эшелонированной защиты для АС;
- принципы и стандарты построения современных автоматизированных систем и подходы к интеграции сетей в автоматизированные системы;
- основные уязвимости и угрозы ИБ для автоматизированных систем;
- основные методы и средства реализации удаленных сетевых атак на автоматизированные системы;
- политики безопасности и меры защиты в автоматизированных системах;
- правовые основы и правила работы программно-аппаратных средств обеспечения ИБ АС;
- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; возможности и способы использования безопасных информационных технологий в работе современного предприятия при практической реализации требований отечественных и международных стандартов ИБ;
- условия создания и эксплуатации программно-аппаратных средств обеспечения ИБ АС;
- безопасные сетевые технологии, в которых используются программно-аппаратные средств обеспечения ИБ.

**уметь:**

- устанавливать операционную систему, устранять ее сбои, устанавливать необходимые драйверы и прикладные программы; выполнять резервирование системной информации;
- устанавливать платы расширения и подключать и конфигурировать различные периферийные устройства;
- администрировать рабочие станции и серверы;
- осуществлять поиск и защиты от компьютерных вирусов и программных закладок;
- работать с технической документацией;
- работать с измерительной и контролирующей техникой.
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенных систем;
- применять комплексный подход к обеспечению ИБ для АС;
- осуществлять управление и администрирование защищенных АС;
- анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным АС;
- определять и устранять основные угрозы ИБ для АС;
- строить модели угроз и нарушителя ИБ для АС и АС;

	<ul style="list-style-type: none"> <li>- выявлять и устранять уязвимости в основных компонентах АС;</li> <li>- обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;</li> <li>- проектировать защищенные АС; применять стандартные решения для защиты информации в АС и квалифицированно оценивать их качество;</li> <li>- используя современные методы и средства, разрабатывать политику ИБ для АС;</li> <li>- реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем;</li> <li>- применять комплексный подход к обеспечению ИС для АС;</li> <li>- осуществлять управление и администрирование защищенных АС;</li> <li>- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе АС с целью обеспечения требуемого уровня ее защищенности;</li> <li>- экономически эффективно использовать программно-аппаратные средства обеспечения ИБ информационных технологий в профессиональной деятельности;</li> <li>- применять в различных проектах программно-аппаратные средства обеспечения ИБ.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>- навыками анализа угроз ИБ и уязвимостей в АС;</li> <li>- навыками распознавания сетевых атак на АС;</li> <li>- навыками разработки политик ИБ для АС;</li> <li>- навыками использования программно-аппаратных средств обеспечения информационной безопасности АС.</li> </ul>	
<b>Б2.П</b>	<b>ПРОИЗВОДСТВЕННАЯ ПРАКТИКА</b>	
<b>Б2.П.1</b>	<p style="text-align: center;"><b>ПРОИЗВОДСТВЕННАЯ-ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ</b></p> <p><b>Цели изучения дисциплины:</b>  Целями производственной практики по 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 общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.</p> <p>Место дисциплины в структуре ООП:  Практика по профилю специальности является вторым этапом производственной (профессиональной) практики и направлена на закрепление, расширение, углубление и систематизацию знаний, полученных при изучении общепрофессиональных и специальных дисциплин, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.</p> <p>Программа практики по специальности обеспечивает обоснованную последовательность формирования у студентов единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.</p>	<b>216(6)</b>

Изучение дисциплины направлено на формирование и развитие следующих компетенций:

- способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
- способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
  - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
  - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
  - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
  - способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);
  - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
  - способностью управлять информационной безопасностью автоматизированной системы (ПК-28);
  - способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);
  - способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);
  - способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);
  - способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах (ПСК-7.4);
  - способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);
- В результате изучения дисциплины студент должен:
- знать:
- основные должностные инструкции инженера-программиста, сетевого администратора; специалиста в области информационных безопасности;
  - краткую характеристику выпускаемой продукции, её технический уровень.
  - взаимосвязь основных цехов и отделов предприятия и систему управления ими, своё место в этой системе;
  - основные задачи, решаемые предприятием по совершенствованию информационной безопасности;
  - действующие на предприятии правила внутреннего распорядка, техники безопасности, пожарной безопасности и режима работы предприятия;
  - характеристики аппаратного и программного обеспечения локальной или корпоративной сети предприятия;
  - принципы администрирования и обслуживания локальной или корпоративной сети предприятия;
  - монтажа электронного оборудования и средств электронных коммуникаций.
  - организационную структуру и функциональную часть автоматизированных систем управления (АСУ);
  - политики безопасности и меры защиты в АС;
  - комплексный подход к построению эшелонированной защиты для АС;
  - принципы и стандарты построения современных автоматизированных систем и подходы к интеграции сетей в автоматизированные системы;
  - основные уязвимости и угрозы ИБ для автоматизированных систем;

- основные методы и средства реализации удаленных сетевых атак на автоматизированные системы;
- политики безопасности и меры защиты в автоматизированных системах;
- правовые основы и правила работы программно-аппаратных средств обеспечения ИБ АС;
- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; возможности и способы использования безопасных информационных технологий в работе современного предприятия при практической реализации требований отечественных и международных стандартов ИБ;
- условия создания и эксплуатации программно-аппаратных средств обеспечения ИБ АС;
- безопасные сетевые технологии, в которых используются программно-аппаратные средства обеспечения ИБ.

уметь:

- устанавливать операционную систему, устранять ее сбои, устанавливать необходимые драйверы и прикладные программы; выполнять резервирование системной информации;
- устанавливать платы расширения и подключать и конфигурировать различные периферийные устройства;
- администрировать рабочие станции и серверы;
- осуществлять поиск и защиты от компьютерных вирусов и программных закладок;
- работать с технической документацией;
- работать с измерительной и контролирующей техникой.
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенных систем;
- применять комплексный подход к обеспечению ИБ для АС;
- осуществлять управление и администрирование защищенных АС;
- анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным АС;
- определять и устранять основные угрозы ИБ для АС;
- строить модели угроз и нарушителя ИБ для АС и АС;
- выявлять и устранять уязвимости в основных компонентах АС;
- обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;
- проектировать защищенные АС; применять стандартные решения для защиты информации в АС и квалифицированно оценивать их качество;
- используя современные методы и средства, разрабатывать политику ИБ для АС;
- реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем;
- применять комплексный подход к обеспечению ИС для АС;
- осуществлять управление и администрирование защищенных АС;
- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе АС с целью обеспечения требуемого уровня ее защищенности;
- экономически эффективно использовать программно-аппаратные средства обеспечения ИБ информационных технологий в профессиональной деятельности;
- применять в различных проектах программно-аппаратные средства обеспечения ИБ.

владеть навыками:

- навыками анализа угроз ИБ и уязвимостей в АС;
- навыками распознавания сетевых атак на АС;
- навыками разработки политик ИБ для АС;
- навыками использования программно-аппаратных средств обеспечения информационной безопасности АС.

<p><b>Б2.П.2</b></p>	<p style="text-align: center;"><b>ПРОИЗВОДСТВЕННАЯ ПРЕДДИПЛОМНАЯ ПРАКТИКА</b></p> <p><b>Цели изучения дисциплины:</b>  Целями производственной–преддипломной практики по 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 общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.</p> <p><b>Место дисциплины в структуре ООП:</b>  Практика по профилю специальности является вторым этапом производственной (профессиональной) практики и направлена на закрепление, расширение, углубление и систематизацию знаний, полученных при изучении общепрофессиональных и специальных дисциплин, на основе изучения деятельности конкретной организации, приобретение первоначального практического опыта.</p> <p>Программа практики по специальности обеспечивает обоснованную последовательность формирования у студентов единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b></p> <ul style="list-style-type: none"> <li>– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);</li> <li>– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);</li> <li>– способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);</li> <li>– способностью создавать и исследовать модели автоматизированных систем (ПК-2);</li> <li>– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);</li> <li>– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);</li> <li>– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);</li> <li>– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);</li> <li>– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);</li> <li>– 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);</li> <li>– способностью участвовать в проектировании системы управления</li> </ul>	<p><b>216(6)</b></p>

информационной безопасностью автоматизированной системы (ПК-12);

- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
- способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
- способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
- способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);
- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);
- способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);
- способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);
- способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5);

**В результате изучения дисциплины студент должен:**

<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- основные должностные инструкции инженера-программиста, сетевого администратора; специалиста в области информационных безопасности;</li> <li>- краткую характеристику выпускаемой продукции, её технический уровень.</li> <li>- взаимосвязь основных цехов и отделов предприятия и систему управления ими, своё место в этой системе;</li> <li>- основные задачи, решаемые предприятием по совершенствованию информационной безопасности;</li> <li>- действующие на предприятии правила внутреннего распорядка, техники безопасности, пожарной безопасности и режима работы предприятия;</li> <li>- характеристики аппаратного и программного обеспечения локальной или корпоративной сети предприятия;</li> <li>- принципы администрирования и обслуживания локальной или корпоративной сети предприятия;</li> <li>- монтажа электронного оборудования и средств электронных коммуникаций.</li> <li>- организационную структуру и функциональную часть автоматизированных систем управления (АСУ);</li> <li>- политики безопасности и меры защиты в АС;</li> <li>- комплексный подход к построению эшелонированной защиты для АС;</li> <li>- принципы и стандарты построения современных автоматизированных систем и подходы к интеграции сетей в автоматизированные системы;</li> <li>- основные уязвимости и угрозы ИБ для автоматизированных систем;</li> <li>- основные методы и средства реализации удаленных сетевых атак на автоматизированные системы;</li> <li>- политики безопасности и меры защиты в автоматизированных системах;</li> <li>- правовые основы и правила работы программно-аппаратных средств обеспечения ИБ АС;</li> <li>- программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; возможности и способы использования безопасных информационных технологий в работе современного предприятия при практической реализации требований отечественных и международных стандартов ИБ;</li> <li>- условия создания и эксплуатации программно-аппаратных средств обеспечения ИБ АС;</li> <li>- безопасные сетевые технологии, в которых используются программно-аппаратные средств обеспечения ИБ.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- устанавливать операционную систему, устранять ее сбои, устанавливать необходимые драйверы и прикладные программы; выполнять резервирование системной информации;</li> <li>- устанавливать платы расширения и подключать и конфигурировать различные периферийные устройства;</li> <li>- администрировать рабочие станции и серверы;</li> <li>- осуществлять поиск и защиты от компьютерных вирусов и программных закладок;</li> <li>- работать с технической документацией;</li> <li>- работать с измерительной и контролирующей техникой.</li> <li>- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенных систем;</li> <li>- применять комплексный подход к обеспечению ИБ для АС;</li> <li>- осуществлять управление и администрирование защищенных АС;</li> <li>- анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным АС;</li> <li>- определять и устранять основные угрозы ИБ для АС;</li> <li>- строить модели угроз и нарушителя ИБ для АС и АС;</li> <li>- выявлять и устранять уязвимости в основных компонентах АС;</li> <li>- обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;</li> </ul>
--



	<ul style="list-style-type: none"> <li>- проектировать защищенные АС; применять стандартные решения для защиты информации в АС и квалифицированно оценивать их качество;</li> <li>- используя современные методы и средства, разрабатывать политику ИБ для АС;</li> <li>- реализовывать системы защиты информации в ОИС в соответствии со стандартами по оценке защищенных систем;</li> <li>- применять комплексный подход к обеспечению ИС для АС;</li> <li>- осуществлять управление и администрирование защищенных АС;</li> <li>- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе АС с целью обеспечения требуемого уровня ее защищенности;</li> <li>- экономически эффективно использовать программно-аппаратные средства обеспечения ИБ информационных технологий в профессиональной деятельности;</li> <li>- применять в различных проектах программно-аппаратные средства обеспечения ИБ.</li> </ul> <p><b>владеть навыками:</b></p> <ul style="list-style-type: none"> <li>-навыками анализа угроз ИБ и уязвимостей в АС;</li> <li>-навыками распознавания сетевых атак на АС;</li> <li>-навыками разработки политик ИБ для АС;</li> <li>-навыками использования программно-аппаратных средств обеспечения информационной безопасности АС.</li> </ul>	
<p><b>ФТД</b></p>	<p><b>ФАКУЛЬТАТИВЫ</b></p>	
<p><b>ФТД.1</b></p>	<p style="text-align: center;"><b>МЕДИАКУЛЬТУРА</b></p> <p><b>Цели изучения дисциплины:</b> Целями освоения дисциплины «Медиакультура» являются:</p> <ul style="list-style-type: none"> <li>- формирование «медийной» грамотности, рефлексивности и критического отношению к продуктам медиа, способности творчески расшифровывать и интерпретировать значения, транслируемые средствами массовой информации;</li> <li>- развитие критического творческого мышления по отношению к системе медиа и медиатекстам.</li> </ul> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- раскрыть сущность медиакультуры;</li> <li>- представить культурные феномены, процессы и практики информационного общества, познакомить студентов с методологией их изучения, с современными критическими теориями медиа, проблематизировать повседневное обращение с его «электронными посредниками» – СМИ и средствами персональной коммуникации.</li> </ul> <p><b>Место дисциплины в структуре ООП:</b> Учебный курс «Медиакультура» входит в цикл факультативных дисциплин данной образовательной программы и призван помочь студентам в изучении различных пластов истории и теории культуры, истории средств коммуникации. Он способствует выработке у студентов критической оценки особенностей различных медиа.</p> <p>Курс предполагает, что студенты уже имеют общую подготовку по культурологии, истории, культуре речи и владеют базовыми навыками социокультурного анализа. Знания, полученные при изучении данной дисциплины будут необходимы студентам при ИГА.</p> <p><b>Изучение дисциплины направлено на формирование и развитие следующих компетенций:</b> <b>ОК-6</b> способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p> <p><b>В результате изучения дисциплины студент должен:</b> <b>знать:</b> К определения медийных понятий и основные теоретические подходы к ним,</p>	<p>36</p>

	<p>называть их структурные характеристики.</p> <p>К сущность и особенности культуры, структуру и функции, исследований, используемых в медиакультуре;</p> <p>К школы и концепции культурологии, формы культуры, основы истории мировой и отечественной культуры;</p> <p>К закономерности культурных процессов, функции культурных институтов и значение культурных норм в жизнедеятельности общества.</p> <p><b>уметь:</b></p> <p>К логически верно, аргументировано и ясно строить устную и письменную речь на русском языке;</p> <p>К ориентироваться в мире культурных норм и ценностей;</p> <p>К использовать в профессиональной деятельности базовые знания, подходы и методы культурологии;</p> <p>К использовать культурные нормы, регулирующие отношение человека к человеку, обществу, окружающей среде, использовать данные знания при разработке социальных проектов и в различных сферах жизнедеятельности.</p> <p>К готовить и редактировать тексты профессионального назначения;</p> <p>К публично представлять собственные и известные научные результаты, вести дискуссии.</p> <p>К <b>владеть навыками:</b></p> <p>К практическим опытом и навыками использования элементов медиакультуры на занятиях в аудитории и на учебной практике;</p> <p>К способами демонстрации умения анализировать ситуацию в СМИ;</p> <p>К методиками обобщения результатов анализа современной медиасреды;</p> <p>К способностью к культурному мышлению, к обобщению и анализу, восприятию информации, навыками поиска информации, выделения значимых единиц в информационных потоках.</p> <p>К способностью к письменной и устной деловой коммуникации;</p> <p>К навыками чтения и перевода текстов по профессиональной тематике на одном из иностранных языков;</p> <p>К навыками ведения дискуссии и выделения значимых единиц в информационных потоках.</p> <p><b>Дисциплина включает в себя следующие разделы:</b></p> <p>Медиагенезис. Феномен медиакультуры. Основные эпохи в развитии медиа и функции медиакультуры. Медиакультура и медиасреда. Медиакультура как феномен эпохи модерна. Медиакультура и мифы XX века. Медиакультура России в эпоху социальной модернизации.</p>	
--	---	--