

**Аннотации дисциплин образовательной программы  
по направлению 10.03.01 «Информационная безопасность»  
Направленность/ профиль «Комплексная защита объектов информатизации»**

Блок I.	Дисциплины (модули)	Аннотации
		Базовая часть
	ИСТОРИЯ РОССИИ	<p>Дисциплина «История России» является базовой частью блока дисциплин учебного плана. Реализуется на факультете управления кафедрами: кафедрой истории России средневековья и нового времени, кафедрой истории России новейшего времени.</p> <p>Цель дисциплины: сформировать у студентов целостное и научно-корректное представление о закономерностях и динамике исторического развития России, о важнейших событиях социально-экономической, политической и культурной жизни страны.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- выявить основные этапы, черты и особенности экономического развития России с древнейших времен до конца XX века</li> <li>- определить особенности социальной структуры общества на различных этапах его развития;</li> <li>- проследить особенности политической системы России с древнейших времен и до начала XXI вв.;</li> <li>- проследить тенденции и факты развития культурной жизни России;</li> <li>- акцентировать внимание обучающихся на дискуссионных проблемах изучения истории России.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-3 - способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма</p> <p>В результате освоения дисциплины «История России» обучающийся должен:</p> <p>Знать: закономерности, основные этапы истории России с древнейших времен до XXI в., историю становления и развития государственности, общие культурно-ценностные ориентиры;</p> <p>Уметь: использовать полученные исторические знания для формирования гражданской позиции;</p> <p>Владеть: навыками реферирования научной литературы по истории России; навыками анализа исторических источников.</p>

		<p>Рабочей программой предусмотрены следующие виды контроля: в форме теста, промежуточная аттестация в форме зачета и экзамена.</p> <p>Общая трудоемкость освоения дисциплины «История России» составляет 4 зачетные единицы.</p>
	<p><b>ВСЕОБЩАЯ ИСТОРИЯ</b></p>	<p>Дисциплина «Всеобщая история» является базовой частью блока дисциплин учебного плана. Реализуется на историко-филологическом факультете кафедрой всеобщей истории.</p> <p>Цель дисциплины - формирование у студентов взгляда на историю как на единый процесс, поле взаимодействия личности, социума, культуры, на выявление соотношения общего и особенного в развитии цивилизаций с целью применения полученных знаний в практической работе, а также в научных исследованиях в данной области.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- рассмотрение основных фактов и явлений всеобщей истории;</li> <li>- выявлении типологических моделей цивилизационного развития;</li> <li>- выделение уникального в историческом процессе;</li> <li>- прослеживание эволюции базовых понятий, необходимых для структурирования событийной канвы мировой истории.</li> <li>- формирование представлений о современных методологических подходах к изучению истории.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-3 - способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>1. Знать:</p> <ul style="list-style-type: none"> <li>- основные этапы истории локальных цивилизаций и содержание основных стадий всемирно-исторического развития от древности до новейшего времени;</li> <li>- различные подходы к изучению истории человеческого общества;</li> <li>- значение гражданских ценностей для развития человеческого общества;</li> <li>- основные методы социальных и гуманитарных наук.</li> </ul> <p>2. Уметь:</p>

		<ul style="list-style-type: none"> <li>- логично и аргументированно излагать свою позицию по различным проблемам общественного развития, выступать публично по исторически значимым проблемам, обосновывать собственную позицию по дискуссионным историческим вопросам;</li> <li>- анализировать, руководствуясь принципами научной объективности и историзма, содержание социально-экономических, политических и культурных процессов в истории.</li> </ul> <p>3. Владеть:</p> <ul style="list-style-type: none"> <li>- навыками проведения комплексного анализа исторических явлений и процессов;</li> <li>- навыками анализа социально значимых исторических явлений и процессов.</li> </ul> <p>По дисциплине предусмотрены следующие виды контроля: в форме теста, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>ФИЗИЧЕСКАЯ КУЛЬТУРА И СПОРТ</b></p>	<p>Дисциплина «Физическая культура и спорт» является частью блока дисциплин учебного плана по направлению подготовки 10.03.01 «Информационная безопасность»</p> <p>Дисциплина реализуется кафедрой физической культуры, спорта и безопасности жизнедеятельности.</p> <p>Цель дисциплины: формирование всесторонне развитой личности и способности направленного использования разнообразных средств и методов физической культуры, спорта и туризма для сохранения и укрепления здоровья обучающихся, развитие психофизических способностей в процессе осознанной двигательной активности и готовности к будущей профессии, формирование здорового образа жизни, приобретение умений, знаний в области физической культуры и спорта.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>- приобретение мотивационных отношений к физической культуре и спорту, установки на здоровый образ жизни, физическое самосовершенствование, потребности к регулярным занятиям физическими упражнениями;</li> <li>- овладение знаниями научно-биологических основ физической культуры и здорового образа жизни;</li> <li>- формирование опыта творческого использования физкультурно-спортивной деятельности для достижения жизненных и профессиональных успехов.</li> </ul>

		<p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-9 - способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- значение физической культуры как фактора развития человеческого капитала, основной составляющей здорового образа жизни;</li> <li>- основные показатели физического развития, функциональной подготовленности и работоспособности и влияние физических упражнений на данные показатели;</li> <li>- основы организации здорового образа жизни;</li> <li>- требования профессиональной деятельности в области физической культуры и спорта к уровню физической подготовленности работников;</li> <li>- правила безопасности при проведении занятий по физической культуре и спорту;</li> <li>- методики обучения технике двигательных действий и развития физических качеств средствами базовых видов спорта;</li> <li>- основы планирования и проведения занятий по физической культуре;</li> <li>- основы контроля и самооценки уровня физической подготовленности по результатам тестирования.</li> <li>- правила эксплуатации контрольно-измерительных приборов и инвентаря</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- самостоятельно оценивать уровень физической подготовленности;</li> <li>- планировать отдельные занятия и циклы занятий по физической культуре оздоровительной направленности с учетом особенностей профессиональной деятельности;</li> <li>- проводить самостоятельные занятия по общей физической подготовке;</li> <li>- определять и учитывать величину нагрузки на занятиях;</li> <li>- соблюдать правила техники безопасности при выполнении упражнений;</li> <li>- пользоваться спортивным инвентарем, оборудованием и контрольно-измерительными приборами и обнаруживать их неисправности.</li> </ul> <p>Владеть: техникой основных двигательных действий базовых видов спорта на уровне выполнения контрольных нормативов; навыками самоконтроля и анализа своего физического</p>
--	--	--

		<p>состояния, физической подготовленности. Рабочей программой предусмотрены следующие виды контроля:</p> <ul style="list-style-type: none"> <li>- текущий контроль успеваемости в форме: основная группа: посещение лекций, выполнение программы практических занятий, контрольная работа,</li> <li>подготовительная группа: посещение лекций, выполнение программы практических занятий с учетом медицинских показаний контрольная работа,</li> <li>специальная медицинская группа (СМГ): посещение лекций, выполнение программы практических занятий с учетом медицинских показаний, контрольная работа;</li> <li>- промежуточная аттестация в форме зачета.</li> </ul> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы</p>
<p>ЭЛЕКТИВНЫЕ ДИСЦИПЛИНЫ ФИЗИЧЕСКОЙ КУЛЬТУРЕ И СПОРТУ</p>	<p>ПО</p>	<p>Элективные дисциплины по физической культуре и спорту являются обязательной частью цикла дисциплин модуля «Физическая культура и спорт» учебного плана для всех направлений подготовки бакалавриата 10.03.01 «Информационная безопасность» профили "Комплексная защита объектов информатизации" "Организация и технология защиты информации".</p> <p>Дисциплина реализуется на кафедре физической культуры, спорта и безопасности жизнедеятельности.</p> <p>Цель дисциплины: Формирование всесторонне развитой личности, способности направленного использования разнообразных средств и методов физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической готовности студента к будущей профессии.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>- приобретение мотивационных отношений к физической культуре, установки на здоровый образ жизни, физическое самосовершенствование, потребности к регулярным занятиям физическими упражнениями;</li> <li>- овладение знаниями научно-биологических основ физической культуры и здорового образа жизни;</li> <li>- формирование опыта творческого использования физкультурно-спортивной деятельности для достижения жизненных и профессиональных успехов.</li> </ul> <p>Элективные дисциплины по физической</p>

		<p>культуре и спорту направлены на формирование следующей компетенции:</p> <ul style="list-style-type: none"> <li>- способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности. (ОК-9)</li> </ul> <p>В результате освоения дисциплины обучающиеся должны:</p> <ul style="list-style-type: none"> <li>- знать научные основы биологии, физиологии, теории и методики педагогики и практики физической культуры и здорового образа жизни, систему практических умений и навыков, обеспечивающих сохранение и укрепление здоровья, развитие и совершенствование психофизических способностей, качеств и свойств личности средствами физической культуры и спорта;</li> <li>- уметь квалифицированно применять приобретенные навыки в своей профессиональной и бытовой деятельности, проводить самостоятельные занятия физическими упражнениями с общей развивающей, профессионально-прикладной и оздоровительно-корректирующей направленностью;</li> <li>- владеть знаниями биологических основ физической культуры и здорового образа жизни, способами определения дозировки физической нагрузки и направленности физических упражнений</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля:</p> <ul style="list-style-type: none"> <li>- текущий контроль осуществляется в течение семестра на методико-практических, учебно-тренировочных занятиях. Объектами оценивания являются: активность на занятиях, выполнения контрольных работ в виде теста, сдачи нормативов физической направленности, своевременность выполнения различных видов заданий, посещаемость всех видов занятий, степень усвоения теоретических знаний, результаты самостоятельной работы.</li> <li>- промежуточная аттестация в форме зачёта.</li> </ul> <p>Общая трудоёмкость дисциплины составляет 328 ч.</p>
	<p><b>ИНОСТРАННЫЙ ЯЗЫК</b></p>	<p>Дисциплина «Иностранный язык» является основной частью блока дисциплин учебного плана. Дисциплина реализуется на ФИСБ ИИНТБ кафедрой иностранных языков.</p> <p>Цель дисциплины: обучение английскому языку – формирование и совершенствование у студентов навыков чтения, говорения,</p>

		<p>аудирования и письма и наличие у выпускников определенных умений (как вторичного средства письменного и устного общения), необходимых для решения задач межличностного и межкультурного взаимодействия на английском языке</p> <p>Задачи дисциплины иностранного языка предполагают развитие у обучающихся следующих сформированных навыков:</p> <p>Чтение:</p> <ul style="list-style-type: none"> <li>- понимать тексты, построенные на частотном языковом материале повседневного и профессионального общения, понимать описание событий, чувств, намерений в письмах;</li> </ul> <p>Аудирование:</p> <ul style="list-style-type: none"> <li>- понимать основные положения четко произнесенных высказываний в пределах литературной нормы на известные темы, с которыми приходится иметь дело на работе, в вузе, на отдыхе и т.д.;</li> <li>- понимать, о чем идет речь в большинстве радио- и телепрограмм о текущих событиях, а также передач, связанных с личными или профессиональными интересами. Речь говорящих должна быть при этом четкой и относительно медленной.</li> </ul> <p>Говорение:</p> <ul style="list-style-type: none"> <li>- уметь без предварительной подготовки участвовать в диалогах на знакомую, интересующую тему;</li> <li>- уметь строить несложные связные высказывания о своих личных впечатлениях, событиях, рассказывать о своих мечтах, надеждах и желаниях;</li> <li>- уметь кратко обосновать и объяснить свои взгляды и намерения;</li> <li>- уметь рассказать историю или изложить сюжет книги или фильма и выразить к этому свое отношение.</li> </ul> <p>Письмо:</p> <ul style="list-style-type: none"> <li>- уметь писать несложные связные тексты на знакомые или интересующие темы.</li> </ul> <p>Дисциплина «Иностранный язык» направлена на формирование следующих компетенций:</p> <p>ОК-7 способность 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>В результате освоения дисциплины «Иностранный язык» обучающийся должен:</p> <p>Знать: - лексические и грамматические основы,</p>
--	--	--

		<p>обеспечивающие коммуникацию общего характера без искажения смысла при письменном и устном общении;</p> <p>Уметь: - оформить свои результаты в письменной и устной форме на иностранном языке;</p> <ul style="list-style-type: none"> <li>- выделять главные мысли, факты, необходимую информацию;</li> <li>- оценивать информацию с точки зрения объективности и достоверности;</li> <li>- грамотно передавать смысл высказывания с иностранного языка на русский.</li> <li>- понимать четко произносимую речь (аутентичную монологическую, диалогическую) повседневной и профессиональной тематики;</li> <li>- сообщать информацию (подготовленное монологическое высказывание); в рамках страноведческой, общенаучной и общетехнической тематики (в объеме не менее 10-12 фраз);</li> <li>- фиксировать информацию, получаемую при чтении текста;</li> </ul> <p>Владеть: - основами письменного перевода с использованием словаря, грамотно передавая смысл высказывания с иностранного языка на русский;</p> <ul style="list-style-type: none"> <li>- навыками ознакомительного, изучающего чтения с возможностью использования словаря;</li> <li>- речевым этикетом повседневного общения (знакомство, представление, установление и поддержание контакта, запрос и сообщение информации, побуждение к действию, выражение просьбы, согласия/несогласия с мнением собеседника, завершение беседы)</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в виде контрольной работы, промежуточная аттестация в форме зачета и экзамена .</p> <p>Общая трудоемкость освоения дисциплины «Иностранный язык» составляет 6 зачетных единиц.</p>
	<p><b>ТЕХНИЧЕСКИЙ ПЕРЕВОД ТЕКСТОВ</b></p>	<p>Дисциплина «Технический перевод текстов» является основной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: обучение умению различать потенциальные грамматические и лексические трудности в контексте при чтении и переводе научной и технической литературы с целью формирования сознательного подхода к</p>



		<p>языковому материалу, навыков работы с оригинальными научно-техническими текстами в соответствии со спецификой направления подготовки.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- дальнейшее расширение терминологической лексики по проблемам защиты информации,</li> <li>- освоение твердо установленных в письменной речи грамматических норм и сложных грамматических конструкций, развитие грамматических навыков распознавания и понимания форм, конструкций, характерных для специального текста на материале научных статей, конференций и семинаров; изучение частотных грамматических явлений, характерных для специальных текстов</li> <li>- работа с текстами разной стилистики научной, научно-популярной и технической литературы;</li> <li>- поиск и осмысление информации в ходе работы с оригинальной литературой, совершенствование навыков и умений ознакомительного и изучающего чтения, освоение фактического материала, связанного с организацией защиты информации стран изучаемого языка;</li> <li>- устный обмен информацией профессионального характера в процессе делового общения, освоение специальной терминологии.</li> <li>- умение вести патентно-библиографический поиск, в первую очередь в сети Интернет;</li> <li>- редактирование переводов, в том числе перевода статей по специальности, сделанных электронным переводчиком;</li> <li>- установление и поддержание деловых (устных и письменных) контактов с зарубежными коллегами.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-7 - способность 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>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- лексические и грамматические основы, обеспечивающие коммуникацию общего характера без искажения смысла при письменном и устном общении;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- оформить свои результаты в письменной и устной форме на иностранном языке;</li> </ul>
--	--	---

		<ul style="list-style-type: none"> <li>- выделять главные мысли, факты, необходимую информацию;</li> <li>- грамотно передавать смысл высказывания с иностранного языка на русский.</li> <li>- понимать четко произносимую речь (аутентичную монологическую, диалогическую) повседневной и профессиональной тематики;</li> <li>- сообщать информацию (подготовленное монологическое высказывание); в рамках страноведческой, общенаучной и общетехнической тематики (в объеме не менее 10-12 фраз);</li> <li>- фиксировать информацию, получаемую при чтении текста;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- основами письменного перевода с использованием словаря, грамотно передавая смысл высказывания с иностранного языка на русский;</li> <li>- навыками ознакомительного, изучающего чтения с возможностью использования словаря.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в виде контрольной работы, промежуточная аттестация в форме зачета и экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.</p>
	<p>СПЕЦИАЛЬНОЕ ДОКУМЕНТОВЕДЕНИЕ И ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ</p>	<p>И</p> <p>Дисциплина «Специальное документоведение и документационное обеспечение управления» является основной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой Информационной безопасности для студентов 2 курса, относится к базовой части блока дисциплин учебного плана.</p> <p>Цель дисциплины: формирование понимания закономерностей образования документов и способов их создания, развития систем документации и систем документирования, рассмотрение документа как объекта защиты и нападения, усвоение технологии эффективного поиска информации по профилю деятельности.</p> <p>Задачи: рассмотрение теоретических и прикладных аспектов документирования информации: свойств, функций и признаков документа, способов и средств документирования, структуры документа, порядка его составления и оформления, методов и способов защиты документа и документированной информации, классификации документов и систем документации, основ документационного</p>

		<p>обеспечения управления.  Дисциплина направлена на формирование следующей компетенции:  ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.  В результате освоения дисциплины обучающийся должен:  Знать основные аспекты создания официальных и служебных документов; принципы организации документооборота; основных нормативных правовых актов Российской Федерации в области документационного обеспечения управления.  Уметь правильно использовать реквизиты организационно-распорядительных документов; создавать формуляр документа; подготавливать организационно-распорядительные документы и информационно-справочные документы.  Владеть навыками работы с документами; навыками подготовки и передачи документов на архивное хранение; навыками работы с документами в соответствии с установленным порядком.  Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в виде практических заданий, промежуточная аттестация в форме зачета.  Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.</p>
	<p>ОСНОВЫ РОССИЙСКОГО ПРАВА</p>	<p>Дисциплина «Основы российского права» является основной частью блока дисциплин учебного плана, реализуется кафедрой теории права и сравнительного правоведения юридического факультета РГГУ.  Цель дисциплины: формирование у обучающихся способности, как познавательно-аналитического, так и практического использования в различных сферах деятельности знаний об основах современного права в целом и специфике важнейших институтов и отраслей российского права в частности.  Задачи:</p> <ul style="list-style-type: none"> <li>• понимание специфики и содержания права как социокультурного явления и его роли в современном обществе;</li> <li>• приобретение обучающимися навыков правового анализа явлений, проблем и процессов современного общества в целях развития способности к самоорганизации и самообразованию;</li> </ul>

		<ul style="list-style-type: none"> <li>• приобретение основных знаний о важнейших правовых отраслях и институтах современной российской системы права;</li> <li>• формирование у обучающихся основ правовой культуры и понимания гуманистической ценности права и прав человека для толерантного восприятия социальных, этнических, конфессиональных и культурных различий;</li> <li>• осознание своих прав и обязанностей человека и гражданина;</li> <li>• развитие способности противодействовать проявлениям коррупционного поведения в сфере своей профессиональной деятельности;</li> <li>• развитие у обучающихся способности применять правовые знания на практике и осуществлять свою профессиональную деятельность с учетом требований норм права.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-4- способностью использовать основы правовых знаний в различных сферах деятельности.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>• специфику и основные принципы права как социокультурного явления и его роль в современном обществе;</li> <li>• специфику основных отраслей и институтов права современного общества и российской системы права;</li> <li>• основы правового регулирования в сфере своей профессиональной деятельности;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>• ориентироваться в системе источников современного права и находить нужную правовую информацию;</li> <li>• осуществлять профессиональную деятельность с учетом требований правовых норм;</li> <li>• противодействовать проявлениям коррупционного поведения в сфере своей профессиональной деятельности;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>• навыками правового анализа проблем и процессов современного общества;</li> <li>• навыками использования правовой информации при решении практических задач в различных сферах своей деятельности.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль</p>
--	--	---

		<p>успеваемости в виде контрольных вопросов и заданий, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p>ЭКОНОМИКА</p>	<p>Дисциплина «Экономика» является основной частью блока дисциплин учебного плана, реализуется на экономическом факультете кафедрой «Теоретическая и прикладная экономика»</p> <p>Цель дисциплины – сформировать у студентов представление об экономическом образе мышления, о предмете и методологии экономической теории и её месте в системе наук, познакомить их с общетеоретическими основами хозяйствования, научить ориентироваться в меняющихся экономических условиях.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>• рассмотреть основные направления развития экономической мысли, современные экономические теории, эволюцию представлений о предмете экономической теории;</li> <li>• дать представление о задачах, функциях и методах экономической науки;</li> <li>• раскрыть сущность и типы общественного воспроизводства, предпосылки компромиссного экономического выбора;</li> <li>• изложить основы и закономерности функционирования экономических систем;</li> <li>• познакомить студентов с понятийно-категориальным аппаратом экономической науки и инструментами экономического анализа;</li> <li>• сформировать у студентов знания о сущности и механизмах функционирования рынка, об основных организационно-правовых формах предпринимательской деятельности и методах оценки результатов деятельности фирмы;</li> <li>• дать четкое представление об основных макроэкономических показателях, инструментах государственной фискальной и денежно-кредитной политики;</li> <li>• сформировать целостное представление об основных тенденциях развития экономики России на современном этапе.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-2 - способность использовать основы экономических знаний в различных сферах деятельности</p> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p>

		<p>Знать:</p> <ul style="list-style-type: none"> <li>• основные направления развития экономической мысли;</li> <li>• сущность и формы организации хозяйственной деятельности;</li> <li>• цели, функции и инструменты экономической политики.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>• определять тенденции развития экономики России на современном этапе;</li> <li>• ориентироваться в системе показателей результатов хозяйственной деятельности на макро- и микроуровнях;</li> <li>• применять графический метод при исследовании экономических взаимосвязей;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>• методами экономического анализа социальных явлений.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в виде контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы.</p>
	МЕНЕДЖМЕНТ	<p>Дисциплина «Менеджмент» является частью базового цикла обязательных дисциплин учебного плана для всех направлений подготовки и всех форм обучения. Дисциплина реализуется кафедрой управления Института управления, экономики и права.</p> <p>Цель курса – формирование у студентов необходимого объема компетенций, требуемых для реализации организаторских и управленческих способностей, позволяющих ускорить их профессиональную адаптацию к деятельности в современных организациях и эффективного взаимодействия с коллективом в рамках актуального правового поля с соблюдением норм профессиональной и общечеловеческой этики, и с учетом последних достижений и передового опыта в области менеджмента.</p> <p>Задачи курса:</p> <ul style="list-style-type: none"> <li>– ознакомить студентов с истоками формирования управленческих идей и взглядов и их дальнейшей эволюцией в разные исторические периоды в различных странах, а также связью современного состояния управленческой мысли с прошлым;</li> <li>– рассмотреть основные аспекты современного менеджмента и дать представление об интегрированном подходе в</li> </ul>

		<p>вопросах концептуальной теории управления и менеджмента, и практики менеджмента в организациях различных форм собственности.</p> <ul style="list-style-type: none"> <li>– ознакомить с внедрением новых принципов и методов эффективного менеджмента и координации деятельности коллективов людей в современных организациях;</li> <li>– ознакомить с внедрением новых принципов и методов управления коллективами людей во имя достижения высоких социально-экономических результатов.</li> <li>– рассмотреть научно-практические подходы и образцы современного управления, доминирующие в той или иной социально-культурной среде, исходя из принципов цивилизованных рыночных отношений.</li> </ul> <p>Дисциплина направлена на формирование следующих универсальных компетенций:</p> <p>ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности.</p> <p>ОК-6 - способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>– эффективность использования стратегии сотрудничества для достижения поставленной цели, определять свою роль в команде (ОК-5).</li> <li>– особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывает их в своей деятельности (ОК-5).</li> <li>– возможности применения своих ресурсов и их пределов (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы (ОК-6).</li> <li>– понимать важность планирования перспективных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда (ОК-6).</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– предвидеть результаты (последствия) личных действий и планировать последовательность шагов для достижения</li> </ul>
--	--	---

		<p>заданного результата (ОК-5);</p> <ul style="list-style-type: none"> <li>- реализовать намеченные цели деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда (ОК-5);</li> <li>- использовать предоставляемые возможности для приобретения новых знаний и навыков (ОК-6).</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- методами эффективного взаимодействия с другими членами команды, в том числе участвует в обмене информацией, знаниями и опытом, и презентации результатов работы команды (ОК-5);</li> <li>- оценкой эффективности использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата (ОК-6).</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования и выполнение практических заданий, промежуточный контроль в форме сдачи зачета с оценкой.</p> <p>Итоговая оценка выставляется в полном соответствии с утверждённой в РГГУ рейтинговой системой контроля знаний.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.</p>
	<p><b>ФИЛОСОФИЯ</b></p>	<p>Дисциплина «Философия» является базовой частью блока дисциплин учебного плана, реализуется на факультете философии кафедрой истории зарубежной философии.</p> <p>Цель дисциплины: формирование способности понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>• овладение базовыми представлениями о ключевых проблемах и основных исторических типах европейской философии;</li> <li>• освоение навыков самостоятельного анализа соответствующих первоисточников;</li> <li>• исследование различных социальных явлений с точки зрения их философского смысла.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-1 - Способность использовать основы философских знаний для формирования мировоззренческой позиции.</p> <p>Знать: центральные категории, идеи и</p>



		<p>персоналии представленных разделов философии; проблематику онтологическую, эпистемологическую, антропологическую и аксиологическую; основные философские школы и направления современности;</p> <p>Уметь: дискутировать, логически верно и аргументировано высказывать собственную позицию; работать с источниками и исследовательской литературой по философии, давать самостоятельную оценку тем или иным направлениям и школам философской мысли; оперировать философскими знаниями в профессиональной деятельности;</p> <p>Владеть: навыками поиска необходимой информации для научного исследования; способностью анализировать социально-значимые процессы; навыками толерантного восприятия социальных и культурных различий.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме самостоятельных работ, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ</b></p>	<p>Дисциплина «Безопасность жизнедеятельности» является базовой частью блока дисциплин учебного плана, реализуется кафедрой физической культуры, спорта и безопасности жизнедеятельности.</p> <p>Задачи:</p> <ol style="list-style-type: none"> <li>1. Изучить характер чрезвычайных ситуаций и их последствия для жизнедеятельности.</li> <li>2. Овладеть правовыми основами безопасности жизнедеятельности при возникновении чрезвычайных ситуаций.</li> <li>3. Подготовить студентов к осознанным действиям в чрезвычайных ситуациях, научить грамотно применять способы защиты жизни и здоровья в сложившейся критической обстановке.</li> <li>4. Сформировать навыки оказания первой помощи населению при ликвидации последствий аварий, катастроф, стихийных бедствий, а также при массовых эпидемиях.</li> </ol> <p>Дисциплина направлена на формирование общекультурных и профессиональных компетенций:</p> <ul style="list-style-type: none"> <li>• владением культурой безопасности и риск-ориентированным мышлением, при котором вопросы безопасности и сохранение окружающей среды рассматриваются в качестве</li> </ul>

		<p>важнейших приоритетов в жизни и деятельности (ОК – 8);</p> <ul style="list-style-type: none"> <li>• готовностью пользоваться основными методами защиты населения от возможных последствий аварий, катастроф, стихийных бедствий (ОПК – 6);</li> <li>• способностью ориентироваться в основных нормативно-правовых актах в области обеспечения безопасности (ОПК – 6);</li> <li>• готовностью использовать знания по организации охраны труда, окружающей среды и безопасности в ЧС (ОК – 8).</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: последствия ЧС и способы действия в сложившейся критической ситуации.</p> <p>Уметь: применять профессиональные знания для минимизации негативных экологических последствий обеспечения безопасности в условиях ЧС при оказании первой помощи пострадавшим в ЧС.</p> <p>Владеть: практическими навыками для обеспечения личной безопасности и окружающих в ЧС.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ОСНОВЫ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ</b></p>	<p>Дисциплина «Основы профессиональной деятельности» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины - обучить основам знаний о содержании профессиональной деятельности по направлению подготовки «Информационная безопасность».</p> <p>Задачи дисциплины: изучить базовые содержательные положения в области информационной безопасности и защиты информации; цели и значение информационной безопасности в современном мире; дать представление студенту о роли и значении получаемой профессии; дать представление о возможных направлениях деятельности специалиста в области информационной безопасности; вести в базовые понятия предмета, объекта, целей и задач изучаемых наук и взаимосвязи между ними; изучить основы</p>

		<p>терминологии, присущей рассматриваемой предметной области.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ОК-6: способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;</li> <li>– ОК-8: способен к самоорганизации и самообразованию.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать функции и роль профессионала в области информационной безопасности; способы поиска и сбора информации с использованием информационных технологий и библиотечных ресурсов.</p> <p>Уметь определять направление поиска информации и анализировать ее на предмет пригодности для решения поставленных профессиональных задач; формулировать научные проблемы, возникающие при организации профессиональной деятельности и предлагать методы их решения.</p> <p>Владеть методологией решения стандартных задач профессиональной деятельности на основе собранной информации; теоретическими и практическими навыками адаптации к специфике учебного процесса в вузе, а также к специфике будущей профессии.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СОЦИАЛЬНЫЕ СЕРВИСЫ И СЕТИ</b></p>	<p>Дисциплина «Гуманитарные аспекты информационной безопасности. Социальные сервисы и сети» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование у обучающихся знаний о различных видах социальных сетевых сервисов, развитие умений и навыков эффективного использования их возможностей в профессиональной деятельности.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>-формирование базовых знаний о сервисах Интернета и специфике социальных сетевых сервисов как современного средства</li> </ul>

		<p>массовой информации и коммуникации;  -выработка у обучающихся практических умений по организации работы с социальными сервисами с учётом обеспечения информационной безопасности;  -формирование навыков самообразования и профессионального совершенствования в сфере обеспечения информационной безопасности при изучении социальных сервисов и работы с ними;  -реализация коммуникативных и технических способностей обучающихся при работе с социальными сервисами.  Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности</li> <li>• ОПК-4 -способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <ul style="list-style-type: none"> <li>- знать: основные особенности Интернета как современной коммуникационной среды, принципы функционирования социальных сервисов в сети Интернет;</li> <li>- уметь: пользоваться основными сервисами Интернета и основными элементами делового общения в сети;</li> <li>- владеть: правилами нетикета при работе в сети Интернет, навыками работы при использовании основных социальных сервисов.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p>ГУМАНИТАРНЫЕ АСПЕКТЫ  ИНФОРМАЦИОННОЙ  БЕЗОПАСНОСТИ.  ИНФОРМАЦИОННОЕ  ПРОТИВОБОРСТВО</p>	<p>Дисциплина (модуль) «Гуманитарные аспекты информационной безопасности. Информационное противоборство» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование у</p>

		<p>обучающихся знаний о сущности информационных войн и информационного оружия, методов и способов их реализации, а также о возможностях информационного противоборства потенциальному противнику.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- раскрытие основных категорий информационной войны и базовых факторов, оказывающих влияние на её содержание;</li> <li>- определение основных принципов, отражающих закономерности информационной войны;</li> <li>- анализ базовых уровней общественного сознания, выступающего в качестве поля сражения;</li> <li>- выявление основных классов и практических видов информационного оружия;</li> <li>- установление базовых мероприятий по предотвращению или нейтрализации последствий применения информационного оружия;</li> <li>- раскрытие практических мероприятий программного характера по защите от информационного оружия.</li> </ul> <p>Дисциплина (модуль) направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;</li> <li>• ОПК-4 - способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li> <li>• ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- базовый понятийный аппарат в области защиты информации, информационных войн и информационного оружия;</li> <li>- основные нормативно-правовые документы в профессиональной деятельности;</li> <li>- состав, классификацию информационного оружия и основные способы его применения;</li> <li>- основные методы и приемы информационного противоборства.</li> </ul>
--	--	---

		<p>Уметь:</p> <ul style="list-style-type: none"> <li>- пользоваться нормативно-правовыми документами в области защиты информации;</li> <li>- применять полученные знания в научно-исследовательской работе;</li> <li>- применять способы и средства защиты информации в условиях информационного противоборства;</li> <li>- ставить цели и выбирать пути эффективного решения задач в области защиты информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками работы с нормативно-правовыми актами в сфере защиты информации;</li> <li>- навыками определения угроз информации применительно к объектам защиты в условиях информационного противоборства;</li> <li>- опытом выявления причин, обстоятельств и условий дестабилизирующего воздействия на защищаемую информацию со стороны источников воздействия;</li> <li>- навыками определения направлений защиты информации с учетом характера защищаемой информации и задач по ее защите.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоёмкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p>МАТЕМАТИЧЕСКИЙ АНАЛИЗ</p>	<p>Дисциплина «Математический анализ» является частью блока дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность, направленность Комплексная защита объектов информатизации. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: обеспечить необходимую фундаментальную подготовку студентов к изучению и усвоению основных идей и методов современных разделов математики. Задачи: обеспечить овладение будущими специалистами современными методами исследования непрерывных процессов, используя понятийный аппарат дифференциального и интегрального исчисления и разработанные в анализе способы вычисления различных количественных характеристик.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-2 - способность применять</li> </ul>

		<p>соответствующий математический аппарат для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: основные понятия, теоремы и методы дифференциального и интегрального исчисления, ряды и их сходимость, разложение элементарных функций в ряд, методы решения дифференциальных уравнений первого и второго порядка, математические модели, в которых используются полученные знания и навыки</p> <p>Уметь: исследовать функции, строить их графики, вычислять производные и интегралы, исследовать ряды на сходимость, находить решения некоторых классов дифференциальных уравнений, самостоятельно решать вычислительные задачи математического анализа с помощью специальных программных средств</p> <p>Владеть: аппаратом дифференциального и интегрального исчисления, навыками решения дифференциальных уравнений первого и второго порядка, навыками работы с библиотеками прикладных программ для решения задач математического анализа.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, тестирования, контрольной работы, расчетно-графической работы, коллоквиума, промежуточная аттестация в форме экзамена (1 семестр) и экзамена (2 семестр).</p> <p>Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц.</p>
	<p>ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА</p>	<p>Дисциплина «Теория вероятностей и математическая статистика» является частью блока дисциплин учебных планов по направлению подготовки 10.03.01 Информационная безопасность, направленность Комплексная защита объектов информатизации. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: формирование базовых представлений о теории вероятностей и математической статистике под углом зрения их практического приложения в различных областях научных исследований и инженерной практики. Задачи: на примере комбинаторной теории вероятностей перейти к общим понятиям теории вероятностей и математической статистики, сформулировать основные теоремы,</p>

		<p>необходимые для понимания смежных дисциплин и практической деятельности.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-2 - способность применять соответствующий математический аппарат для решения профессиональных задач.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: случайные события и случайные величины, законы распределения; закон больших чисел, методы статистического анализа</p> <p>Уметь: вычислять вероятности случайных событий, составлять и исследовать функции распределения случайных величин, определять числовые характеристики случайных величин; обрабатывать статистическую информацию для оценки значений параметров и проверки значимости гипотез</p> <p>Владеть: вероятностным подходом к постановке и решению задач, навыками работы с библиотеками прикладных программ для решения вероятностных и статистических задач.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, тестирования, контрольной работы, контроля выполнения внеаудиторных заданий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.</p>
	<p>ДИСКРЕТНАЯ МАТЕМАТИКА</p>	<p>Дисциплина «Дискретная математика» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: формирование у студентов теоретических знаний и практических навыков по применению методов дискретной математики в процессе решения прикладных задач. Задачи: ознакомление с различными направлениями и методологией дискретной математики; обучение студентов теории и практике применения методов дискретной математики для поиска и обоснования решений в различных областях экономики и управления.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-2 - способность применять соответствующий математический аппарат для решения профессиональных задач;</li> </ul>



		<p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: методы теории множеств, математической логики, алгебры высказываний, теории графов, теории автоматов, теории алгоритмов, формулы комбинаторики, индуктивное определение формулы, булевы функции, принцип двойственности, методы построения СДНФ, СКНФ и полинома Жегалкина, определение полноты и замкнутости, понятия изоморфизма и планарности графов.</p> <p>Уметь: использовать свойства операций над множествами, строить булевы функции в задачах, которые сформулированы на обычном языке, переводить лингвистические конструкции в логические формулы и наоборот, применять логические формулы для анализа ситуаций, выраженных на обычном языке, определять фундаментальные свойства булевых функций, строить СДНФ и СКНФ, строить многочлен Жегалкина, строить диаграмму Мура для функций, строить граф, соответствующий изучаемой математической задаче, алгебраически распознавать важнейшие свойства графов.</p> <p>Владеть: комбинаторным, теоретико-множественным подходами к постановке и решению задач; навыками моделирования прикладных задач методами дискретной математики.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме устного опроса, участия в дискуссии на практическом занятии, коллоквиума, контрольной работы, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>ТЕОРИЯ ИНФОРМАЦИИ</p>	<p>Дисциплина «Теория информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность(профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.) кафедрой комплексной защиты информации.)</p> <p>Цель дисциплины– формирование у студентов</p>

		<p>основных понятий, утверждений, и обучение основным методам, принципам и приёмам теории информации, которые играют базовую роль в моделировании процессов и решении разнообразных теоретических и научно-практических задач, возникающих при передаче сигналов и хранении информации.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>• обучить студентов основным понятиям теории информации;</li> <li>• сформировать у студентов математический подход к решению практических задач, связанных с профессиональной деятельностью;</li> <li>• привить студентам навыки для перехода от постановки задачи к математической модели;</li> <li>• научить решать основополагающие теоретико-информационные задачи профессиональной направленности с применением необходимого математического аппарата;</li> <li>• подготовить студентов к овладению основным математическим аппаратом, требуемым для дальнейшего построения систем эффективной передачи и обработки информации.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>знать: основные виды и формы представления информации, теорему В.А.Котельникова и другие основополагающие теоремы теории информации, её фундаментальные положения и проблемы передачи информации, основные подходы, методы и приёмы для определения количества информации, основные общие принципы кодирования и декодирования информации, основные особенности и характеристики передачи информации, основные подходы для повышения помехозащищённости и достоверности передачи и приёма данных;</p> <p>уметь: применять свойство аддитивности информации, использовать формулу Шеннона во взаимосвязи с другими базовыми понятиями теории информации, использовать различные основные способы кодирования информации при решении задач, связанных с профессиональной деятельностью;</p> <p>владеть: основными подходами к постановке и</p>
--	--	--

		<p>решению задач, навыками математического описания на основе теории информации прикладных задач, связанных с профессиональной деятельностью, навыками расчета скорости передачи информации и пропускной способности канала связи при отсутствии и наличии помех.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме теста и контрольной работы, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p>ФИЗИКА</p>	<p>Дисциплина Б1.Б.17 «Физика» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 1-го курса во 2-ом семестре и 2-го курса в 3-ем семестре, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой Комплексной защиты информации.</p> <p>Содержание дисциплины охватывает основные разделы общей физики.</p> <p>Цель дисциплины: помочь освоению современной физической картины мира и методов научного познания природы, формирование навыков использования физического аппарата в профессиональной деятельности.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– ознакомить с физическими законами, лежащими в основе процессов кодирования информации в сигналах, способах хранения, обработки, хранения, передачи и приема сигналов;</li> <li>– обучить методам подхода к решению физических задач;</li> <li>– привить навыки планирования, выполнения и обработки результатов физического эксперимента;</li> <li>– ознакомить с физическими моделями и принципами работы технических устройств;</li> <li>– дать навыки использования современных информационных технологий для поиска, приобретения и переработки информации физического содержания и оценки ее достоверности.</li> </ul> <p>В соответствии ФГОС ВП по направлению</p>

		<p>подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) дисциплина «Физика» направлена на формирование следующей общепрофессиональной компетенции</p> <ul style="list-style-type: none"> <li>– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>знать:</p> <ul style="list-style-type: none"> <li>– основные понятия, законы и модели механики;</li> <li>– основные понятия, законы и модели электричества и магнетизма;</li> <li>– основные понятия, законы и модели теории колебаний и волн, оптики;</li> <li>– особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности;</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>– применять физический подход при решении практических задач;</li> <li>– применять полученные знания при освоении последующих базовых дисциплин, спецкурсов</li> <li>– применять полученные при решении практических задач организации защиты информации на объектах;</li> </ul> <p>владеть:</p> <ul style="list-style-type: none"> <li>– навыками проведения физического эксперимента и обработки его результатов.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, защиты лабораторных работ, промежуточная аттестация в форме письменной контрольной работы, зачета во 2-ом семестре и экзамена в 3-м семестре.</p> <p>Общая трудоемкость освоения дисциплины составляет 7 зачетные единицы.</p>
	<p>ЭЛЕКТРОТЕХНИКА</p>	<p>Дисциплина «Электротехника» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: формирование у студента</p>

		<p>понимания сущности законов электротехники, методов расчета и анализа электрических цепей в практической работе по организации технической защиты информации и в научных исследованиях в данной области.</p> <p>Задачи: изучение основных методов анализа и расчета электрических цепей различной сложности; ознакомление с современными методами расчета электрических цепей, основанными на компьютерных технологиях; формирование навыков, необходимых для самостоятельного решения проблемы технической защиты информации путем представления реальной ситуации в виде электрической схемы замещения.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-3 способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные понятия и законы электротехники; основы теории расчета и анализа электрических и магнитных цепей постоянного и переменного тока; принципы действия и основные характеристики электромагнитных устройств и электрических машин; принципы действия и характеристики простейших электротехнических и полупроводниковых элементов и устройств; основные понятия в области электрических измерений; основы эксплуатации электроприборов, электротехнических и электронных устройств, а также основы электробезопасности.</p> <p>Уметь читать и собирать простейшие электрические схемы, понимая физические процессы, протекающие в электроустановках; пользоваться основными электрическими измерительными приборами; правильно выбирать наиболее рациональные методы расчета и анализа электромагнитных процессов в электрических и магнитных цепях;</p> <p>Владеть навыками чтения электронных схем; навыками безопасного использования технических средств в профессиональной деятельности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета с оценкой.</p>
--	--	---

		Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы
	ЭЛЕКТРОНИКА СХЕМОТЕХНИКА И	<p>Дисциплина «Электроника и схемотехника» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: профессиональная подготовка будущих специалистов в области элементной базы радио-электронной аппаратуры.</p> <p>Задачи: формирование специальных физических, математических, теоретических и практических знаний, которые обеспечили бы возможность понимать и анализировать процессы в радиоэлектронных цепях систем обработки информации; привитие навыков в использовании методов анализа базовых элементов и микроэлектронных устройств, применяемых в системах передачи и обработки информации; приобретение опыта использования элементной базы радиоэлектронной аппаратуры; формирование способности к самостоятельному и инициативному решению технических проблем; обучение основам элементной базы полупроводниковой электроники, схемотехники электронных аналоговых устройств, схемотехники электронных цифровых устройств, схемотехники смешанных аналогово-цифровых устройств, устройств отображения информации.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-3 способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные понятия и законы электротехники и схемотехники; принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы схемотехники современной радиоэлектронной аппаратуры; основы эксплуатации электроприборов, электротехнических и электронных устройств, а также основы электробезопасности.</p> <p>Уметь проводить расчёты типовых аналоговых и</p>

		<p>цифровых узлов радиоэлектронной аппаратуры; пользоваться основными электрическими измерительными приборами.</p> <p>Владеть навыками проектирования и расчёта простейших аналоговых и цифровых схем; навыками безопасного использования технических средств в профессиональной деятельности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.</p>
	<p>ИНФОРМАТИКА</p>	<p>Дисциплина «Информатика» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цели дисциплины: Формирование у обучающихся основных понятий информатики и современной информационной культуры, формирование устойчивых навыков работы на персональном компьютере в условиях локальных и глобальных вычислительных сетей и систем телекоммуникации, развитие навыков применения информационных технологий для решения задач организационной, управленческой и научно-технической деятельности.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>• изучение студентами основных понятий теории информации и кодирования;</li> <li>• изучение студентами систем счисления и методов представления данных в ЭВМ;</li> <li>• изучение студентами типовых свойств и способов задания булевых функций;</li> <li>• освоение студентами арифметических операций в дополнительном коде;</li> <li>• ознакомление студентов с конструкцией ЭВМ;</li> <li>• освоение студентами прикладных и системных программных средств, предназначенных</li> <li>• для реализации современных информационных технологий;</li> <li>• изучение студентами основных возможностей вычислительных сетей;</li> <li>• изучение студентами основ защиты информации.</li> </ul>

		<p>Дисциплина (модуль) направлена на формирование следующих компетенций: ОПК-4 (способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации).</p> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>1. знать:</p> <ul style="list-style-type: none"> <li>- цели, задачи, место данной дисциплины среди других дисциплин, основные понятия, предмет и структуру информатики, информационных технологий;</li> <li>- теоретические основы информатики;</li> <li>- правила преобразования чисел из одной системы счисления в другую, правила выполнения арифметических и логических операций.</li> </ul> <p>2. уметь:</p> <ul style="list-style-type: none"> <li>- использовать в профессиональной деятельности возможности вычислительной техники и программного обеспечения;</li> <li>- использовать ресурсы Интернет;</li> <li>- работать с прикладным и системным программным обеспечением.</li> </ul> <p>3. владеть:</p> <ul style="list-style-type: none"> <li>- методами поиска, хранения и обработки информации;</li> <li>- основными методами работы с современным системным и прикладным программным обеспечением;</li> <li>- навыками работы в компьютерной сети Интернет.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса на практическом занятии, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины (модуля) составляет 3 зачетные единицы.</p>
	<p><b>ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ</b></p>	<p>Дисциплина «ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРОВАНИЯ» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности института информационных наук и технологий безопасности РГГУ, кафедрой информационных технологий и систем.</p> <p>Цель дисциплины – приобретение знаний, навыков и умений в области технологий и методов программирования, а также освоение основных алгоритмов обработки и хранения больших данных.</p>



		<p>Задачи дисциплины:</p> <ol style="list-style-type: none"> <li>1. Изучение базовых принципов программирования на языке высокого уровня;</li> <li>2. Дать широко применяемые технологии и методы программирования на языках C/C++, в том числе, специализированные методы обработки и хранения данных;</li> <li>3. Изучение главных управляющих структур языков C/C++;</li> <li>4. Изучение принципов объектно-ориентированного программирования;</li> <li>5. Сформировать навыки и умения по разработке алгоритмов в задачах последовательного и объектно-ориентированного программирования;</li> <li>6. Познакомить со стандартами языков C/C++ и их отличительными особенностями;</li> <li>7. Дать представления о процедуре отладки разрабатываемых приложений;</li> <li>8. Сформировать представления о разработке эффективных приложений и обучить основным методам оптимизации;</li> <li>9. Дать представление о разработке реляционных баз данных;</li> <li>10. Обучить основам построения самообучающихся алгоритмов на языках высокого уровня</li> </ol> <p>Дисциплина (модуль) направлена на формирование следующей компетенции:</p> <p>ОПК-2 - Способность применять соответствующий математический аппарат для решения профессиональных задач</p> <p>ОПК-3 - Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач</p> <p>Знать: базовых принципов программирования на языке высокого уровня; главные управляющих структур языков C/C++; принципы объектно-ориентированного программирования; алгоритмы отладки разрабатываемых приложений; методы разработки эффективных приложений и оптимизации по времени и памяти; основы построения самообучающихся алгоритмов; специализированные методы обработки и хранения данных.</p> <p>Уметь: применять специализированные методы обработки и хранения данных на языках C/C++; разрабатывать алгоритмы для решения задач последовательного и объектно-ориентированного программирования; применять принципы объектно-ориентированного программирования для</p>
--	--	---

		<p>построения высоко эффективных приложений; разрабатывать простейшие модели реляционных баз данных на языках высокого уровня C/C++;</p> <p>Владеть: базовыми принципами программирования на языке высокого уровня; методами оптимизации разрабатываемых алгоритмов по затрачиваемому машинному времени на исполнение программы и используемой памяти компьютера; основными управляющими структурами языков C/C++;</p> <p>методами сортировки и хранения данных; методами и подходами к динамическому выделению памяти в пространстве памяти компьютера.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических работ, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ЯЗЫКИ ПРОГРАММИРОВАНИЯ</b></p>	<p>Дисциплина «ЯЗЫКИ ПРОГРАММИРОВАНИЯ» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности института информационных наук и технологий безопасности РГГУ, кафедрой информационных технологий и систем.</p> <p>Цель дисциплины – приобретение знаний, навыков и умений в области высокоуровневых языков программирования, а также освоение современных алгоритмов анализа больших данных.</p> <p>Задачи дисциплины:</p> <ol style="list-style-type: none"> <li>1. Изучение базовых принципов программирования на языке высокого уровня Python;</li> <li>2. Изучение специализированных технологий и методов программирования на языках C/C++ и Python для анализа и хранения данных;</li> <li>3. Изучение главных управляющих структур языков Python;</li> <li>4. Изучение функционального программирования на языке Python;</li> <li>5. Приобретение навыков и умений по разработке алгоритмов в задачах анализа данных с использованием библиотеки Scikit-Learn;</li> <li>6. Формирование навыков работы в программной библиотеке TensorFlow;</li> <li>7. Приобретение навыков работы в среде PyCharm и Jupyter;</li> </ol>

		<p>8. Сформировать представления о разработке эффективных приложений;</p> <p>9. Дать представление о методике исследования больших данных;</p> <p>10. Обучить основам построения самообучающихся алгоритмов на языке Python;</p> <p>Дисциплина (модуль) направлена на формирование следующей компетенции:</p> <p>ОПК-2 - Способность применять соответствующий математический аппарат для решения профессиональных задач.</p> <p>ОПК-7 - Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</p> <p>Знать: базовых принципов программирования на языке высокого уровня Python; главные управляющих структур языков Python; принципы объектно-ориентированного программирования; алгоритмы отладки разрабатываемых приложений; методы разработки эффективных приложений и оптимизации по времени и памяти; основы построения самообучающихся алгоритмов; специализированные методы обработки и хранения данных.</p> <p>Уметь: применять специализированные методы обработки и хранения данных на языке Python; разрабатывать алгоритмы для решения задач последовательного и объектно-ориентированного программирования; применять принципы объектно-ориентированного программирования для построения высоко эффективных приложений;</p> <p>Владеть: базовыми принципами программирования на языке высокого уровня; методами оптимизации разрабатываемых алгоритмов по затрачиваемому машинному времени на исполнение программы и используемой памяти компьютера; основными управляющими структурами языков Python; методами сортировки и хранения данных; методами и подходами к динамическому выделению памяти в пространстве памяти компьютера.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических работ, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины</p>
--	--	---

	<p>ЛИНЕЙНАЯ АЛГЕБРА И АНАЛИТИЧЕСКАЯ ГЕОМЕТРИЯ</p>	<p>составляет 4 зачетных единиц.</p> <p>Дисциплина «Линейная алгебра и аналитическая геометрия» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: подготовить специалистов, обладающих знаниями достижений классической математики, способных применять полученные знания в области информатики.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- обеспечить уровень математической грамотности студентов, достаточный для формирования навыков математической постановки и решения классических оптимизационных задач и моделирования процессов;</li> <li>- научить студентов применять основные понятия и методы линейной алгебры и аналитической геометрии для расчета различных количественных характеристик в задачах экономической теории и теории управления;</li> <li>- сформировать у студентов навыки использования математических методов линейной алгебры и аналитической геометрии при моделировании сложных процессов и принятии оптимальных управленческих решений;</li> <li>- научить студентов использовать геометрическую интерпретацию типичных задач экономической теории и теории управления в практической деятельности.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-2 - способность применять соответствующий математический аппарат для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- базовые понятия и основные технические приемы линейной алгебры и аналитической геометрии и теории линейных пространств;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- использовать алгоритмические приемы решения стандартных задач;</li> <li>- применять математический аппарат при решении типовых задач;</li> <li>- формулировать основные теоремы линейной алгебры и аналитической геометрии;</li> </ul>
--	---	--

		<p>Владеть:</p> <ul style="list-style-type: none"> <li>- стандартными методами и моделями линейной алгебры и аналитической геометрии и их применением к решению прикладных задач;</li> <li>- навыками математической формализации прикладных задач, анализа и интерпретации решений соответствующих математических моделей.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольных работ, коллоквиума, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц.</p>
	<p><b>АППАРАТНЫЕ СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ</b></p>	<p>Дисциплина «Аппаратные средства вычислительной техники» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 1-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: приобретение знаний и умений, необходимых для деятельности, связанной с эксплуатацией и обслуживанием современных средств вычислительной техники, а так же подготовка обучаемых к грамотному и эффективному использованию компьютера как инструмента для решения задач различной степени сложности в области компьютерной безопасности.</p> <p>Задачи: изучение основ и элементной базы вычислительной техники; изучение принципов построения и функционирования комбинационных схем и цифровых автоматов; изучение принципов работы микропроцессорных систем, архитектуры и принципов работы ЭВМ; формирование навыков, необходимых для управления аппаратными средствами на низ-ком уровне.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-3 - способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.</p> <p>В результате освоения дисциплины обучающийся должен:</p>

		<p>Знать принципы работы базовых элементов и устройств компьютеров; логические основы вычислительной техники и архитектуру основных типов современных аппаратных средств; основные понятия и законы электротехники; структуру и принципы работы современных и перспективных микропроцессоров; состав и назначение функциональных компонентов компьютера.</p> <p>Уметь управлять компьютером, используя особенности работы базовых элементов и устройств компьютеров.</p> <p>Владеть методикой настройки и поиска неисправностей программно-аппаратных и технических средств; навыками безопасного использования технических средств в профессиональной деятельности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических занятий, промежуточная аттестация в форме зачета.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.</p>
	<p><b>СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Сети и системы передачи информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: теоретическое изучение и практическое освоение принципов построения и функционирования современных сетей и систем передачи данных.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>– формирование знаний в области выбора, анализа и применения сетей и систем передачи данных;</li> <li>– уяснение основных понятий и определений передачи информации, эталонной модели взаимодействия открытых систем (модель ISO/OSI, модель TCP/IP), архитектуры и средств взаимодействия процессов в сетях;</li> <li>– рассмотрение современных тенденций развития сетей связи.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p>

		<p>ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.);</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: основные принципы построения, архитектуру и топологию современных ЛВС, технологии Ethernet (FastEthernet, GigabitEthernet), TokenRing, FDDI-стандарты, принципы работы, сравнительные характеристики, преимущества и недостатки, основные средства построения современных ЛВС, классификации, внутреннюю архитектуру, режимы работы, протоколы сетевого уровня модели ISO/OSI; мульти-сервисные сети, технологии передачи голосового трафика VoIP, IP-телефонии.</p> <p>Уметь: настраивать базовые настройки сетевых устройств 2-го и 3-го уровня; обнаруживать ошибки в настройке маршрутизации; уметь пользоваться научно технической литературой в области компьютерных сетей.</p> <p>Владеть: базовой терминологией по дисциплине, навыками настройки и эксплуатации коммуникационного оборудования.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практического занятия, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы</p>
	<p><b>ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p>Дисциплина «Основы информационной безопасности» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Целью курса является формирование знаний о совокупности проблем в сфере науки, техники и технологий, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, понимания основных принципов, направлений и методов обеспечения информационной безопасности.</p> <p>Задачи: анализ вопросов, связанных с сущностью и значением информационной безопасности, её местом в системе национальной безопасности,</p>

		<p>определением теоретических, концептуальных, методологических и организационных основ обеспечения безопасности объектов информатизации, анализом методов и средств защиты информации.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"><li>– ОК-5: способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;</li><li>– ОПК-4: способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li><li>– ОПК-7: способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li></ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные понятия в области информационной безопасности и защиты информации; базовые содержательные положения в области информационной безопасности и защиты информации; современную доктрину информационной безопасности; цели и принципы защиты информации;</p> <p>Уметь выявлять факторы, влияющие на защиту информации; устанавливать структуры угроз защищаемой информации; устанавливать и раскрывать сущности компонентов защиты информации; раскрывать назначения, сущности и структуры систем защиты информации; ставить цели и выбирать пути эффективного решения задач в области информационной безопасности;</p> <p>Владеть классификацией защищаемой информации по видам тайны; умению анализировать существующие угрозы информационной безопасности и пути их нейтрализации и устранения; подходами к созданию комплекса мер по защите информации предприятия; навыками подбора, изучения и</p>
--	--	--



		<p>обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности. Рабочей программой предусмотрены следующие виды контроля: Текущий контроль:</p> <ul style="list-style-type: none"> <li>- опрос (устный или письменный)</li> <li>- участие в дискуссии на семинаре</li> <li>- контрольная работа</li> <li>- тестирование</li> <li>- реферат,</li> </ul> <p>Промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p>Дисциплина «Правовое обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».</p> <p>Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.</p> <p>Цель курса: сформировать взгляд на правовое обеспечение информационной безопасности как на системную научно-практическую деятельность, одну из основ которой составляет работа по нормативно-правовому обеспечению информационной безопасности.</p> <p>Задачи курса:</p> <ul style="list-style-type: none"> <li>- изучить конституционные гарантии прав граждан на доступ к информации, в том числе права свободно искать, получать, передавать, производить и распространять информацию любым законным способом с учетом особенностей реализации этих прав в отношении информации ограниченного доступа;</li> <li>- освоить основы правового регулирования отношений в информационной сфере, меры и средства организационно-правового обеспечения информационной безопасности и защиты информации ограниченного доступа, в том числе основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации;</li> <li>- рассмотреть понятие тайны как правового режима ограничения доступа к информации, в том числе правового режима государственной тайны и иных видов тайн, особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан;</li> </ul>

		<p>- изучить правовые основы и порядок сертификации средств защиты информации и практику правового регулирования лицензионной деятельности в области информационной безопасности и защиты информации ограниченного доступа.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности</p> <p>ОПК-5 - способностью использовать нормативные правовые акты в профессиональной деятельности</p> <p>ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p>Дисциплина «Организационное обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».</p> <p>Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.</p> <p>Цель курса: формирование знаний по теоретическим и практическим проблемам функционирования систем организационного и правового обеспечения информационной безопасности с целью формирования практических навыков по организационной защите информации и применению норм права в области информационной безопасности. Способствовать в подготовке специалиста, умеющего сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.</p> <p>Задачи курса:</p>

		<ul style="list-style-type: none"> <li>- изучить базовые теоретические понятия, лежащие в основе мероприятий по организационному и правовому обеспечению информационной безопасности;</li> <li>- овладеть практическими организационными методами защиты информации на объектах информатизации;</li> <li>- овладеть необходимой юридической терминологией;</li> <li>- сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-5 - способностью использовать нормативные правовые акты в профессиональной деятельности</p> <p>ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p> <p>Для изучения данной дисциплины, в результате освоения предшествующих дисциплин, обучающийся должен:</p> <ul style="list-style-type: none"> <li>- понимать сущность информации, методы и способы её отражения и передачи;</li> <li>- знать виды носителей информации и особенности фиксации на них информации;</li> <li>- представлять угрозы защищаемой информации, методы и способы её защиты;</li> <li>- знать основы информационного права, сущность конфиденциальности информации;</li> <li>- понимать процессы управленческой деятельностью.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.</p>
	<p><b>ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Техническая защита информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению</p>

		<p>подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий обеспечения безопасности информации от ее утечки по техническим каналам.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>• получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности информации от утечки по техническим каналам;</li> <li>• изучение теоретических основ информационной безопасности на объектах информатизации;</li> <li>• формирование умений использовать основные достижения в области защиты информации от утечки по техническим каналам при реализации своей профессиональной деятельности;</li> <li>• владение практическими навыками защиты информации на объектах информатизации;</li> <li>• развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-1 – способность анализировать физические явления и процессы для решения профессиональных задач</li> <li>• ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</li> <li>• ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: основные понятия, связанных с</p>
--	--	--

		<p>обеспечением защитой информации от ее утечки по техническим каналам, цели и задачи предметной области, сущность технической защиты информации и ее место среди других направлений обеспечения информационной безопасности, технические средства и методы по добыванию информации, методы, способы и технические решения по технической защите информации (ТЗИ), порядок построения ТЗИ, показатели эффективности защиты и методы их оценки, основные руководящие, методические и нормативные документы по технической защите информации.</p> <p>Уметь: описывать (моделировать) объекты защиты, выявлять и оценивать угрозы безопасности информации на конкретных объектах, использовать системный подход к исследованию и построению ТЗИ, определять рациональные меры защиты на объектах и оценивать их эффективность, контролировать эффективность мер технической защиты информации.</p> <p>Владеть: комплексным подходом к построению ТЗИ, навыками по выявлению возможных каналов утечки информации, решения задачи по проектированию и обслуживанию системы защиты информации (СЗИ) на объектах информатизации с использованием типовых проектных решений и стандартов.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов и лабораторных работ, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.</p>
	<p><b>КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Криптографические методы защиты информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: получение основных знаний об использовании криптографических методов для защиты информации при ее хранении, обработке и дистанционной передаче электронных данных.</p> <p>Задачи: овладение студентами основными криптографическими понятиями, умение студентами: решать типовые криптографические задачи, востребованные практикой; работать со специальной криптографической литературой и нормативными документами; использовать</p>

		<p>полученные знания для решения прикладных задач современной криптографии.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-2 – способностью применять соответствующий математический аппарат для решения профессиональных задач;</p> <p>ОПК-4 – способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</p> <p>ОПК-5 – способностью использовать нормативные правовые акты в профессиональной деятельности.</p> <p>В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:</p> <p>знать:</p> <p>математические модели кодирования систем информации;</p> <p>основные модели, методы и средства криптографической защиты информации;</p> <p>уметь:</p> <p>решать типовые криптографические задачи защиты информации;</p> <p>применять информационные технологии для поиска и обработки информации;</p> <p>владеть:</p> <p>навыками поиска нужной информации в нормативных базах и источниках;</p> <p>навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем электронного документооборота;</p> <p>методами синтеза и анализа криптографических систем и протоколов, способами решения криптографических задач защиты информации в различных сферах человеческой деятельности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, реферата, тестирования, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.ОСНОВНАЯ ЧАСТЬ</p>	<p>Дисциплина «Программно-аппаратные средства защиты информации. Основная часть» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по</p>

		<p>программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: развить у слушателей подход к решению технических задач программно-аппаратной защиты информации.</p> <p>Задачи: изучение основ построения подсистем информационной безопасности, освоение принципов использования программно-аппаратных средств защиты информации, выработка умений проведения оценки защищенности информационных систем.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-3 – должен обладать способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач.</li> <li>• ОПК-4 – должен обладать способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</li> <li>• ОПК-7 – должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; протоколы локальной и сетевой аутентификации; линейку программно-аппаратных средств защиты информации; подходы к тестированию программно-аппаратных средств защиты информации.</p> <p>Уметь осуществлять настройку политики ученой записей, выполнять администрирование учетных записей пользователей на платформах Windows и Linux, идентифицировать слабые места и уязвимости подсистемы идентификации и аутентификации; разрабатывать матрицу разграничения доступа, реализовывать</p>
--	--	---

		<p>дискреционное разграничение доступа к объектам файловой системы и системного реестра; осуществлять выбор программно-аппаратных средств защиты информации адекватных решаемым задачам; составлять методики испытаний средств защиты информации.</p> <p>Владеть навыками администрирования подсистем безопасности, настройки системы управления учетными записями; навыками установки, настройки и эксплуатации средств защиты информации; навыками проверки работоспособности программно-аппаратных средств защиты информации, проведения функционального тестирования средств защиты информации; навыками организовать мероприятия по охране труда и технике безопасности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов и практических заданий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p>ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ, ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ</p>	<p>Дисциплина «Программно-аппаратные средства защиты информации. Межсетевое экранирование, обнаружение вторжений» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Дисциплина реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации</p> <p>Цель дисциплины: ознакомление студентов с основными понятиями в области меж сетевого экранирования и систем обнаружения вторжения; осознание понимания места данных механизмов в общей архитектуре подсистемы защиты информации информационной системы; формирование навыков установки, настройки и реконфигурирования этих средств защиты информации; знакомство с нормативно-методической базой в части их применения.</p>



		<p>Задачи:</p> <ul style="list-style-type: none"> <li>– изучение принципов фильтрации информационных потоков на границе сетей, идентификационных признаков потенциально опасных информационных потоков, сигнатур сетевых атак (вторжений), систем пакетной фильтрации, критериев фильтрации пакетов, управления информационными потоками посредством фильтрации, сопряжения и совместной эксплуатации систем межсетевого экранирования и систем обнаружения вторжений.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-3 – способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач.</li> <li>• ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: требования, предъявляемые к системам межсетевого экранирования и обнаружения вторжения отечественной нормативно-методической базой; базовые функции и место в общей системе информационной безопасности; архитектуру и принципы функционирования межсетевых экранов и систем обнаружения вторжений; назначение и сущность контрольных проверок систем фильтрации пакетов и систем обнаружения вторжений</p> <p>Уметь: осуществлять установку и настройку типовых систем межсетевого экранирования и обнаружения вторжений как уровня узла, так и уровня сети; выполнять настройку систем пакетной фильтрации, встроенных в коммуникационное оборудование.</p> <p>Владеть: навыками оценки сетевого трафика с целью выделения потенциально опасных информационных потоков; навыками определения признаков потенциально опасных потоков и формирования правил межсетевого экранирования, такие потоки исключаящих.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и лабораторных работ, промежуточная аттестация в форме экзамена.</p>
--	--	---

		<p>Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.</p>
	<p><b>ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ</b></p>	<p>Дисциплина «Основы управления информационной безопасностью» относится к базовой части блока дисциплин учебного плана и реализуется на факультете Информационных систем и безопасности кафедрой Информационной безопасности.</p> <p>Цель дисциплины: формирование знаний о процессах управления всеми средствами защиты информации.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>-освоение знаний об архитектуре управления информационной безопасностью корпоративной информационной системы;</li> <li>-приобретение практических навыков по использованию соответствующих нормативно-правовых документов и программных инструментариев для управления ИБ.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li> <li>• ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- как определить виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;</li> <li>-как организовать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;</li> <li>- как формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и экономической</li> </ul>

		<p>целесообразности.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;</li> <li>- применять комплексный подход к обеспечению информационной безопасности;</li> <li>- собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- методами выявления угроз безопасности информации;</li> <li>- навыками организации работы малого коллектива исполнителей с учетом требований защиты информации;</li> <li>- навыками организации работы малого коллектива исполнителей с учетом требований защиты информации.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме дискуссии и практических заданий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.</p>
	<p>КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ. ОРГАНИЗАЦИОННОЕ ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ</p>	<p>Дисциплина «Комплексное обеспечение безопасности объекта информатизации» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Целью курса является формирование представлений о теоретических и методологических основах организационного проектирования, порядка построения, оценки и совершенствования систем защиты информации предприятия (организации).</p> <p>Задачи: рассмотрение сущности и задач организационного проектирования систем защиты информации, методов исследования, принципов организации проектирования и этапов разработки проекта, технологию организации проектных работ.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ОПК-5: способен использовать нормативные правовые акты в профессиональной деятельности;</li> <li>– ОПК-7: способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры</li> </ul>

		<p>и содержания информационных процессов и особенностей функционирования объекта защиты.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать методы, технологию и принципы проектирования систем защиты информации;</p> <p>Уметь проводить предпроектное обследование, проводить анализ экономической целесообразности проектирования систем защиты информации; разрабатывать документы, необходимые для внедрения и функционирования системы защиты информации.</p> <p>Владеть методикой определения структурного построения и состава системы защиты информации и разработкой организационно-нормативных документов, регламентирующих деятельность системы.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, дискуссии и контрольной работы, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ. УПРАВЛЕНИЕ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Комплексное обеспечение безопасности объекта информатизации. Управление службой защиты информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины - создание у студентов представления о структуре службы защиты информации, принципах организации этой службы, о методах организации и управления службой защиты информации в качестве основного звена систем защиты информации.</p> <p>Задачи дисциплины: определение места службы защиты информации в системе безопасности предприятия; описание функций службы защиты информации; описание методов определения оптимальной структуры и штатного состава службы защиты информации применительно к специфике ее функций; описание методов установление организационных основ и принципов деятельности службы защиты информации; описание методов подхода к общим и специфическим вопросам подбора и расстановки кадров, обучения, организации труда сотрудников службы защиты информации;</p>

		<p>анализ методов и технологии управления службой защиты информации.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ОПК-5: способен использовать нормативные правовые акты в профессиональной деятельности;</li> <li>– ОПК-7: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать нормативно-правовые основы организации и управления службой защиты информации; назначение и роль службы защиты информации; основные задачи и функции службы защиты информации.</p> <p>Уметь поддерживать функционирование службы защиты информации на основе нормативно-правовой документации; определять оптимальную структуру службы защиты информации; организовывать и обеспечивать создание службы защиты информации.</p> <p>Владеть навыками организации службы защиты информации на предприятии; навыками разработки нормативных и методических документов по организации и функционированию службы защиты информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, дискуссии и доклада, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>РУССКИЙ ЯЗЫК И КУЛЬТУРА РЕЧИ</p>	<p>Дисциплина «Русский язык и культура речи» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой медиаречи.</p> <p>Цель дисциплины: формирование у студентов целостного комплекса лингвистических знаний, способствующих повышению качества вербальной коммуникации.</p> <ul style="list-style-type: none"> <li>– Задачи:</li> <li>– дать студентам представление о природе, структуре, законах функционирования и развития человеческого языка, его роли в</li> </ul>

		<p>общественной жизни;</p> <ul style="list-style-type: none"> <li>– охарактеризовать современный русский литературный язык как отражение истории и культуры народа, важнейшее условие национальной самоидентификации;</li> <li>– рассмотреть современный русский литературный язык как систему фонетических, словообразовательных, лексических и грамматических средств, с помощью которых могут достигаться различные коммуникативные цели;</li> <li>– углубить знания студентов в области норм русского литературного языка;</li> <li>– обеспечить условия для сознательного восприятия и оценки общественно-речевой практики;</li> <li>– обучить студентов методике использования словарей, справочных и нормативных изданий.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОК-6 способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;</li> <li>• ОК-7 способность 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;</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать концепции социальных, этнических, конфессиональных и культурных различий, толерантного поведения, основ командообразования и проектной деятельности, основ конфликтологии и методов разрешения конфликтов; основные свойства и особенности устройства языка как важнейшего средства человеческого общения; особенности таких форм речи, как устная и письменная, монологическая и диалогическая, подготовленная и спонтанная; факторы, влияющие на выбор речевых средств; историю формирования, генетические связи русского языка, его положение на лингвистической карте мира; понятие нормы литературного языка, ее важнейшие свойства; основные тенденции эволюции литературной нормы; фонетические, лексические, грамматические, семантические, стилистические нормы современного русского языка в целом и применительно к практике официального общения, в том числе в профессиональной и</p>
--	--	---

		<p>научной сфере; языковое законодательство Российской Федерации; словарно-справочную литературу, кодифицирующую нормы современного русского литературного языка и, в частности, издания, адресованные работникам СМИ;.....</p> <p>Уметь взаимодействовать с представителями иных социальных, этнических, конфессиональных и культурных групп, работать в коллективе по решению конкретных проектных задач, содействовать конструктивному взаимодействию в процессе совместной деятельности по решению проектных задач, использовать способы и методы преодоления конфликтных ситуаций; учитывать специфику применения языковых норм в практике официальной и научной, в том числе профессиональной речи; следовать правилам литературного языка в профессиональной деятельности; самостоятельно с помощью словарно-справочной литературы решать вопросы, связанные с определением нормативности различных речевых явлений; руководствоваться в своей профессиональной деятельности правовыми нормами;</p> <p>Владеть навыками толерантного поведения, командной работы, реализации совместных творческих проектов, предупреждения и конструктивного разрешения конфликтных ситуаций в процессе совместной деятельности; навыками устной и письменной речи, ее нормами и средствами выразительности; методиками анализа языковых явлений в структурно-семантическом и коммуникативно-прагматическом аспекте; приемами работы с лингвистическими словарями и справочниками.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, дискуссии и контрольных работ, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ. ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ</b></p>	<p>Дисциплина «Информационные процессы и системы. Вычислительные сети» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой Информационных технологий и систем.</p> <p>Цель дисциплины – формирование систематизированного представления об информационных процессах и системах.</p>

		<p>Получение практической подготовки в области выбора и применения вычислительных сетей для задач автоматизации обработки информации и управления, программирования в современных сетевых средах.</p> <p>Задачи дисциплины: получение практической подготовки в области выбора и применения информационных процессов и вычислительных сетей для задач автоматизации обработки информации и управления.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПСК – 3.2 - способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты.</li> <li>• ОПК - 4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: теоретические основы порождения, функционирования информационных процессов и систем, терминологию и задачи информационных систем; основы работы в информационных системах, общие принципы организации информационных систем разного уровня, особенности различных информационных систем; общие приемы работы с информационными системами, архитектуру вычислительных сетей.</p> <p>Уметь: выбирать различные методы обработки информации в сфере своей деятельности; выбирать информационные системы для реализации задач обработки; планировать использование ИС в рамках поставленных задач; работать с базами данных; использовать знания по архитектуре вычислительных сетей для грамотной работы с ними, выбирать архитектуру вычислительных сетей в соответствии с требованиями к условиям применения.</p> <p>Владеть: современными методами обработки и передачи информации; умениями самостоятельно определять способы решения информационных задач и использовать для этого современные информационные продукты, навыками работы с различными</p>
--	--	---



		<p>вычислительными сетями; практическими навыками проектирования и реализации вычислительных сетей.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, практических работ, теста и реферата, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.</p>
	<p>МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ</p>	<p>Дисциплина «Математическая логика и теория алгоритмов» является частью блока дисциплин учебного плана по направлению подготовки 10.03.01 Информационная безопасность, направленность Комплексная защита объектов информатизации. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.</p> <p>Цель дисциплины: формирование у студентов базовых представлений о теории множеств, общей теории формальных исчислений, теории алгоритмов и теории доказательств. Задачи: студенты должны усвоить основные понятия и теоремы теории множеств, логики высказываний и предикатов, исчисления высказываний и предикатов, а также теории алгоритмов.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-2 - способность применять соответствующий математический аппарат для решения профессиональных задач;</li> <li>• ПК-11 - способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;</li> <li>• ПСК-3.1 - способность проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: основные понятия математической логики и теории множеств, логико-математические языки, логические законы, формальные аксиоматические теории, машины Тьюринга, Тезис Чёрча, рекурсивные и рекурсивно-перечислимые множества и предикаты, примитивно-рекурсивные функции</p> <p>Уметь: применять математический аппарат при решении типовых задач, а также обнаруживать</p>

		<p>применимость аппарата математической логики для решения задач из родственных областей науки и ее приложений</p> <p>Владеть: способностью и готовностью к изучению дальнейших понятий и теорий, разработанных в современной математической логике, а также к оценке степени адекватности предлагаемого аппарата к решению прикладных задач.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, расчетно-графической работы, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ</b></p>	<p>Дисциплина «Информационные технологии. Автоматизированные системы» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой Информационных технологий и ресурсов.</p> <p>Цель дисциплины – овладение основными понятиями системного анализа; понятиями о структуре автоматизированной информационной системе (АИС); об истории создания и развития АИС; о стадиях жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, кодирование, тестирование, установка и сопровождение; а также о технологиях проектирования АИС, оценке и управлении качеством АИС; автоматизации управления групповой разработкой проектов АИС; классификации АИС (по функциональному назначению, по степени сложности, по масштабу применения и т.д.).</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>• Получения студентами представлений о понятиях системного анализа, автоматизированной информационной системе.</li> <li>• Выработки системы знаний о структуре автоматизированной информационной системы.</li> <li>• Приобретение навыков по разработке и моделированию автоматизированных информационных систем.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПСК – 3.2. - способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-</li> </ul>

		<p>экономическое обоснование предлагаемых мер защиты.</p> <ul style="list-style-type: none"> <li>ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: понятия автоматизированных информационных систем; характеристики информационных систем, виды информационных систем, назначение информационных систем; структуру АИС, процессы и стадии жизненного цикла АИС, принципы и этапы проектирования информационных систем, требования к основным ресурсам для реализации проекта информационной систем.</p> <p>Уметь: выбирать необходимые аппаратные и программные средства, подходящие для конкретных потребностей информационной системы, анализировать, моделировать и проектировать информационные системы различной архитектуры.</p> <p>Владеть: Методиками моделирования и проектирования различных автоматизированных систем.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, практических и контрольных работ, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. АДМИНИСТРИРОВАНИЕ ПОДСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Информационные технологии. Администрирование подсистем защиты информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: ознакомление студентов с методами формирования комплексной системы информационной безопасности; овладение методами проектирования и поддержки жизненного цикла систем информационной безопасности, формирование практических</p>

		<p>навыков по управлению и администрированию как отдельными компонентами, так и подсистемой защиты информации в целом, а также по разработке и внедрению предложений по оптимизации комплекса средств защиты информации.</p> <p>Задачи: рассмотрение базовых понятий в области жизненного цикла подсистемы защиты информации; элементы проектирования подсистемы защиты информации, разработка модели угроз и модели нарушителя, построение и последующая эксплуатация подсистемы защиты информации с учётом этих моделей; определения принципов администрирования подсистемы защиты информации, зоны ответственности и обязанностей администратора информационной безопасности; формирование понимания сложности задачи интеграции подсистемы защиты информационной безопасности в информационную систему и администрирования её без ущерба для целевой функции системы.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"><li>• ОПК-4 – способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</li><li>• ПСК-3.2 – способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты.</li><li>• ПК-3 – способность администрировать подсистемы информационной безопасности объекта защиты.</li><li>• ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</li><li>• ПК-12 – способность принимать участие в проведении экспериментальных исследований системы защиты информации</li></ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать состав подсистем защиты информации, принципы их функционирования и особенности работы с ними; методологические и технологические принципы формирования и</p>
--	--	---

		<p>эксплуатации подсистемы защиты информации информационной системы; требования, предъявляемые к подсистеме защиты информации в нормативно-методической документации, методы и способы администрирования подсистемы защиты информации; методики оценки надёжности её функционирования; методы проверки работоспособности подсистем защит информации.</p> <p>Уметь осуществлять выбор и настройку подсистем защиты информации в соответствии с решаемыми задачами, проводить оценку надёжности их функционирования; выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализированных наложенных; участвовать в разработке моделей угроз и нарушителей, учитывать положения моделей при администрировании комплекса средств защиты информации; выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализированных наложенных; выполнять проверку функционирования подсистем защиты информации.</p> <p>Владеть навыками установки, настройки и администрирования подсистем защиты информации, а также модернизации комплекса средств защиты информации; управления сопряжением и совместной эксплуатацией разнородных средств защиты информации; навыками тестирования и оценки эффективности работы подсистем защиты информации документального сопровождения действий по эксплуатации и администрированию комплекса средств защиты информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практических занятий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.</p>
	<p>ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ</p>	<p>Дисциплина «Техническое регулирование в области защиты информации» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной</p>

		<p>защиты информации.</p> <p>Цель дисциплины – формирование систематизированных знаний о вопросах технического регулирования в области защиты информации.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– сформировать знания о лицензировании деятельности в области защиты информации;</li> <li>– сформировать представления о сертификации средств защиты информации;</li> <li>– сформировать и развить компетенции, знания и практические навыки в проведении аттестации объектов информатизации по требованиям безопасности информации.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-7 - способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</li> <li>• ПСК-3.3 - способностью участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты</li> <li>• ПСК-3.4 - способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСТЭК и ФСБ в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; понятия сертификации средств защиты информации; понятия лицензирования в области защиты информации.</p> <p>Уметь пользоваться нормативными документами по защите информации; применять отечественные стандарты в области компьютерной безопасности.</p> <p>Владеть навыками работы с нормативными правовыми актами.</p>
--	--	---

		<p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических занятий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётных единицы.</p>
	<p><b>ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ</b></p>	<p>Дисциплина «Защита информационных процессов в автоматизированных системах» является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины – формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– овладение методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;</li> <li>– формирование навыков анализа информационной инфраструктуры информационных систем и ее безопасности.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-3 - способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач</li> <li>• ПСК-3.1 - способностью проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей</li> <li>• ПСК-3.3 - способностью участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.</p> <p>Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и</p>

		<p>зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.</p> <p>Владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических работ, промежуточная аттестация в форме зачета.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётных единицы.</p>
	<p><b>ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ</b></p>	<p>Дисциплина «Технические средства охраны» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки –№ 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>• получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;</li> <li>• изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;</li> <li>• формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;</li> <li>• владение практическими навыками, применения современных методами, сил и средств в обеспечении безопасности объекта охраны от физического доступа посторонних</li> </ul>



		<p>лиц;</p> <ul style="list-style-type: none"><li>• развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.</li></ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-3 – способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач</p> <p>ПСК-3.3 – способность участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты</p> <p>ПСК-3.4 – способность организовать контроль защищённости объекта информатизации в соответствии с нормативными документами</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: основные понятия и законы электротехники и схемотехники; принципы работы элементов, основы схемотехники современных систем охраны; требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны; состав и порядок разработки нормативных документов по обеспечению безопасности объектов охраны; источники угроз, угрозы, методы поведения нарушителя, методы и средства защиты объектов охраны от физического доступа посторонних лиц; основные принципы и методы по осуществлению контроля, виды и порядок проведения контроля.</p> <p>Уметь: выбирать технические средства охраны для выполнения профессиональных задач; пользоваться основными электрическими измерительными приборами; разрабатывать нормативные документы по обеспечению безопасности объектов охраны от физического доступа посторонних лиц; организовать работу по обеспечению безопасности объектов охраны от воздействия источников угроз и реализации угроз; проводить анализ состояния системы защиты объекта охраны и разрабатывать требования к системе от физического доступа посторонних лиц;</p> <p>анализировать и контролировать уровень организационной и технологической защищённости объекта охраны.</p>
--	--	--

		<p>Владеть: навыками проектирования систем охраны; навыками безопасного использования технических средств в профессиональной деятельности; практическими навыками по использованию нормативных и руководящих документов в организации работ по защите объектов охраны; навыками по моделированию источников угроз и угроз безопасности объектов охраны; навыками по применению стандартов и руководящих документов по защите объектов охраны;</p> <p>практическими навыками работы с инструментальными средствами контроля состояния безопасности объекта охраны.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практического задания, промежуточная аттестация в форме зачёта с оценкой.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p><b>ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ</b></p>	<p>Дисциплина Проектирование систем защиты объектов информатизации является базовой частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;</li> <li>– сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;</li> <li>– сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.</li> </ul> <p>Дисциплина направлена на формирование</p>

		<p>следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности</li> <li>• ОПК-7 - способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</li> <li>• ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</li> <li>• ПСК-3.2 - способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать технологию определения состава защищаемых информационных ресурсов.</p> <p>Уметь проводить обследование объектов информатизации и документировать его результаты.</p> <p>Владеть методами и инструментами обследования объектов информатизации и анализа их защищенности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических занятий, промежуточная аттестация в форме зачета.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.</p>
	<p><b>ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ОПЕРАЦИОННЫЕ СИСТЕМЫ.</b></p>	<p>Дисциплина «Информационные технологии. Операционные системы» является базовой частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой Информационных технологий и систем.</p> <p>Цель дисциплины – формирование у обучающихся общепрофессиональных и профессиональных компетенций, направленных на приобретение способности устанавливать программное и аппаратное обеспечение для</p>

		<p>информационных и автоматизированных систем, способности разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием, способности разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования, а также приобретения практических навыков и умений, необходимых для научно-исследовательской и проектно-конструкторской деятельности.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>• Получения студентами представлений о составе и функциях операционных систем (ОС), их архитектуре и классификации, основных понятиях и определениях.</li> <li>• Выработки системы знаний о принципах построения ОС, вычислительных процессах и ресурсах.</li> <li>• Получения студентами представления об организации локальных и глобальных сетей с использованием ОС.</li> <li>• Приобретение навыков по конфигурированию, администрированию, защите и управлению процессами ОС.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК - 4 - Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</li> <li>• ОПК - 7 - Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: особенности, назначение, функции и архитектуру операционных систем, влияние различных ОС, используемых в современных информационных системах на организацию вычислительного процесса, теоретические сведения о создании и внедрении в рабочий процесс программно-аппаратных комплексов.</p> <p>Уметь: Определять предметную область изучения, предлагать способы реализации прикладных программных сред, предлагать способы управления задачами ОС, разрабатывать</p>
--	--	--

		<p>техническое задание на оснащение отделов, лабораторий и офисов компьютерным и сетевым оборудованием.</p> <p>Владеть: информацией о составе и функциях ОС, методами и средствами выбора оптимальной ОС для решения задач автоматизированной обработки данных конкретной предметной области, способностью устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем, навыками разработки компонентов аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, практической и контрольных работ, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц.</p>
	<p>Вариативная часть</p>	
	<p><b>ФУНКЦИОНАЛЬНЫЙ ПРОЦЕСС И ОРГАНИЗАЦИЯ ПРЕДПРИЯТИЯ</b></p>	<p>Дисциплина (модуль) «Функциональный процесс и организация предприятия» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование у студентов знаний и понимания, что эффективное функционирование современного предприятия и его оптимальная структура могут быть обеспечены только по результатам анализа процессов, протекающих как внутри предприятия, так и при его взаимодействии с внешней средой.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- формирование системы знаний по закономерностям развития предприятий различного типа и организации их функционирования с целью достижения максимальной эффективности при минимальных затратах;</li> <li>- анализ среды, в которой функционирует предприятие, построение моделей функционирования предприятий;</li> <li>- проведение структурного анализа предприятия, выявление соотношения вертикальных и горизонтальных связей, освоения общенаучных</li> </ul>

		<p>методов управления предприятиями.  Дисциплина (модуль) направлена на формирование следующей компетенции:</p> <ul style="list-style-type: none"> <li>• ОПК-7 - способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> <li>• ПК-13 - способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- основные принципы формирования и функционирования предприятий;</li> <li>- принципы управления предприятиями различных форм собственности;</li> <li>- методы анализа внешней и внутренней среды предприятия.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- анализировать структуру предприятий в условиях централизованного и децентрализованного управления;</li> <li>- определять стратегически наиболее эффективные в конкретной ситуации механизмы принятия решений, методы организации коммуникаций и межгруппового поведения.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками анализа структуры и функционирования предприятия;</li> <li>- навыками выработки механизмов принятия решений, направленных на обеспечение эффективного функционирования предприятия в высоко конкурентной среде.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>СОЦИАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p>Дисциплина (модуль) «Социальные аспекты информационной безопасности» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной</p>

		<p>безопасности.</p> <p>Цель дисциплины (модуля) - формирование культуры информационной безопасности (ИБ) в социальной среде.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- изучение основных угроз ИБ в социальной среде;</li> <li>- формирование знаний у обучающихся о правовых и организационных принципах обеспечения ИБ в социальной среде;</li> <li>- выработка у обучающихся практических умений по использованию методов обеспечения ИБ.</li> </ul> <p>Дисциплина (модуль) направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;</li> <li>• ПК-13 - способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- организацию проведения и сопровождение аттестации объекта на соответствие требованиям государственных нормативных документов;</li> <li>- особенности формирования личности, общества и государства, основанного на безопасном стиле жизнедеятельности;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;</li> <li>- комплексно анализировать основные факты и явления, характеризующие знания о социальной безопасности;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками работы с нормативно-правовыми документами;</li> <li>- навыками использования нормативных документов, регламентирующих ИБ.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
--	--	---

<p>МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ</p>	<p>Дисциплина «Математические основы защиты информации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: обучение студентов основным принципам и подходам к использованию математического аппарата для криптографической и комплексной защиты информации.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>• научить определять и учитывать качественные и количественные особенности составляющих криптографической и комплексной защиты информации;</li> <li>• сформировать у студентов представления о механизмах смены параметров криптографической защиты;</li> <li>• научить решать основополагающие теоретико-практические задачи защиты информации с применением необходимого математического аппарата и сформировать математический подход к их решению;</li> <li>• ознакомить студентов с математическими основами криптографических методов защиты компьютерной информации;</li> <li>• ознакомить студентов с основными математическими принципами алгоритмов создания электронной цифровой подписи;</li> <li>• ознакомить студентов с основными принципами построения систем комплексной защиты информации.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ОПК-2 – способность применять соответствующий математический аппарат для решения профессиональных задач.</p> <p>ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>1) знать: основные понятия, методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты</p>
--	---



		<p>информации;</p> <p>2) уметь: применять основные методы, принципы, подходы, алгоритмы и приёмы криптографии и комплексной защиты информации с необходимыми формулами для решения профессиональных математических задач;</p> <p>3) владеть: основными подходами к постановке и решению задач, навыками математического описания профессиональных прикладных задач.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме теста, промежуточная аттестация в форме зачёта.</p> <p>Общая трудоемкость дисциплины составляет 2 зачётные единицы.</p>
	<p><b>ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина Б1.В.04 «Физические основы защиты информации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой Комплексной защиты информации.</p> <p>Цель дисциплины: изучение физических особенностей информативных сигналов акустической, электромагнитной, оптической и ядерной природы, являющихся основой для формирования технических каналов утечки информации, а также, формирование у студентов специализированной физико-технической базы знаний, позволяющей будущим специалистам понимать физические принципы функционирования средств технической разведки и защиты информации. Кроме того, целью дисциплины является развитие в процессе обучения физического мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.</p> <p>Задачи дисциплины: дать знания</p> <ul style="list-style-type: none"> <li>– по физическим принципам и техническим основам формирования и функционирования акустических (речевых) каналов утечки информации;</li> <li>– по физическим принципам и техническим основам формирования и функционирования утечки информации на основе побочных</li> </ul>

		<p>электромагнитных излучений и наводкам;</p> <ul style="list-style-type: none"> <li>– по физическим принципам и техническим основам формирования и функционирования оптических каналов утечки информации;</li> <li>– по физическим принципам и техническим основам формирования и функционирования каналов утечки информации на базе ядерных излучений;</li> </ul> <p>В соответствии ФГОС ВП по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) дисциплина «Физические основы защиты информации» направлена на формирование следующих общепрофессиональных и профессиональных компетенций</p> <ul style="list-style-type: none"> <li>– способностью анализировать физические явления и процессы для решения профессиональных задач (ОПК-1)</li> <li>– способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>знать:</p> <ul style="list-style-type: none"> <li>– основные свойства и особенности распространения акустических и электромагнитных волн и потоков радиоактивных излучений;</li> <li>– основы акустики помещений, человеческой речи и слуха;</li> <li>– принципы электромагнитного экранирования и звукоизоляции помещений;</li> <li>– принципы работы и устройства источников и приемников электромагнитных, звуковых волн и потоков радиоактивных излучений.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>– применять полученные знания при освоении последующих базовых дисциплин, спецкурсов и при решении практических задач организации защиты информации на объектах;</li> <li>– делать обоснованные выводы по результатам измерений;</li> <li>– самостоятельно работать с технической и справочной литературой;</li> </ul> <p>владеть:</p>
--	--	---

		<p>– методами проведения физических измерений, методами корректной оценки погрешностей измерений и расчетов;</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, защиты лабораторных работ, промежуточная аттестация в форме письменной контрольной работы, зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>БАЗЫ ДАННЫХ, СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ</p>	<p>Дисциплина «Базы данных, системы управления базами данных» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: приобретение знаний и умений, необходимых для деятельности, связанной с созданием, управлением и использованием баз данных, а также подготовка обучающихся к грамотному и эффективному использованию баз данных для решения задач в области компьютерной безопасности.</p> <p>Задачи: освоение вопросов построения системы обработки баз данных, создание базы данных, моделирование базы данных, проектирование баз данных в рамках модели «сущность-связь», рассмотрение реляционной модели и нормализации, преобразование моделей «сущность-связь» в реляционные конструкции, реляционная алгебра, язык SQL, проектирование приложений баз данных, администрирование баз данных.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-7 – способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать различные типы баз данных, способы моделирования баз данных, принципы проектирования баз данных, основы построения реляционных баз данных.</p>

		<p>Уметь проектировать базы данных, создавать базы данных на основе проектов, эффективно управлять базами данных, устанавливать, тестировать и использовать программные средства вычислительных и информационных систем, выбирать необходимые инструментальные средства для разработки, создания и управления базами данных;</p> <p>Владеть профессиональной терминологией, методами решения задач управления процессами обработки информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практического занятия, промежуточная аттестация в форме экзамена и курсовой работы.</p> <p>Общая трудоёмкость освоения дисциплины составляет 6 зачётных единиц.</p>
	<p><b>БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ</b></p>	<p>Дисциплина «Безопасность критически важных информационных систем» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: научить студентов приемам работы с инфраструктурой критически важных информационных систем.</p> <p>Задачи: формирование у студентов представлений об инфраструктуре критически важных информационных систем, научить студентов использовать механизмы обеспечения юридической значимости документов.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-4 – должен обладать способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</li> <li>• ПК-15 – должен обладать способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p>

		<p>Знать основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа, нормативные правовые документы в области защиты информации, математические модели безопасности и формальные модели доступа систем, модели и методы защиты операционных систем, основные проектные решения, средства и методы защиты информации от несанкционированного доступа.</p> <p>Уметь решать типовые задачи с помощью методов защиты информации от несанкционированного доступа, применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений; применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия, применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования; уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты.</p> <p>Владеть методами разработки и использования защищенных программных средств; навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах; навыками по реализации политик информационной безопасности.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практического задания, промежуточная аттестация в форме зачёта.</p> <p>Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.</p>
	<p><b>СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЕ ДОСТУПОМ</b></p>	<p>Дисциплина «Системы контроля и управления доступом» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и</p>

технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц с использованием системы контроля и управления доступом (СКУД).

Задачи:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
- владение практическими навыками, применения современных методов, сил и средств контроля и управления доступом в обеспечении безопасности объекта охраны от физического доступа посторонних лиц;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3 – способность администрировать подсистемы информационной безопасности объекта защиты.
- ПК-6 – способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

В результате освоения дисциплины обучающийся должен:

Знать: требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны от доступа посторонних лиц.

Уметь: анализировать состояние безопасности объекта охраны, разрабатывать нормативные документы по созданию и эксплуатации системы охраны объекта.

Владеть: навыками по использованию нормативных и руководящих документов в

		<p>организации работ по защите объектов охраны. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических работ и опроса, промежуточная аттестация в форме зачёта. Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.</p>
	<p><b>БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ</b></p>	<p>Дисциплина «Безопасность операционных систем» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 2-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: научить студентов использовать для решения профессиональных задач современные средства программно-аппаратной защиты информации.</p> <p>Задачи: формирование у студентов представлений о механизмах защиты ОС, выработка умений настраивать функций безопасности ОС, научить студентов использовать встроенные средства защиты информации ОС.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-3 – должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты</li> <li>• ПК-6 – должен обладать способностью принимать участие в проведении проверок работоспособности и эффективности средств защиты информации.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать место средств защиты информации в современных ОС, принципы реализации механизмов идентификации и аутентификации субъектов доступа в ОС, принципы разграничения доступа к объектам в ОС, принципы организации регистрации событий безопасности в ОС.</p> <p>Уметь определять источники и угрозы информационной безопасности в ОС, разрабатывать меры по защите от идентифицированных угроз, выбирать, устанавливать и настраивать средства защиты информации ОС, принимать участие в</p>

		<p>разработке политики безопасности; составлять и реализовывать планы тестирующих мероприятий, имитировать внешние и внутренние атаки нарушения системы безопасности.</p> <p>Владеть профессиональной терминологией, навыками настройки и эксплуатации встроенных средствах защиты информации ОС; навыками эксплуатации и тестирования программно-аппаратных, криптографических и технических средств защиты информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и лабораторных заданий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p>СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА</p>	<p>Дисциплина «Системы электронного документооборота» является вариативной частью блока дисциплин учебного плана, реализует в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.</p> <p>Дисциплина «Системы электронного документооборота» входит в вариативную часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность» профиля «Комплексная защита объектов информатизации».</p> <p>Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.</p> <p>Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением процесса организации электронного документооборота на предприятии различных масштабов и сфер деятельности на примере системы «ДЕЛО», разработанной компанией «Электронные Офисные Системы» (ЭОС), изучением теоретических, методологических и практических проблем, охватывающих обеспечение автоматизации процессов делопроизводства и ведение полностью</p>



		<p>электронного документооборота на объекте информатизации. Направлено на приобретение студентами глубоких и всесторонних знаний по современным методам автоматизированной обработки конфиденциальных документов с обеспечением юридической значимости обрабатываемой информации.</p> <p>Дисциплина направлена на формирование следующих компетенций выпускника:</p> <p>ОПК-4 - способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p> <p>ПК-13 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p> <p>ПСК-3.3. - способностью участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>• сущность информации, методы и способы её отражения и передачи;</li> <li>• основы информационного права, сущность конфиденциальности информации и знать виды носителей информации и особенности фиксации на них информации;</li> <li>• закономерности развития предприятий различного типа и организацию их функционирования с целью достижения максимальной эффективности при минимальных затратах ресурсов;</li> <li>• особенности и характеристики документов аналогового и электронного видов;</li> <li>• методы защиты информации и технологии обработки информации.</li> <li>• виды и особенности рисков, порождаемых системами документооборота;</li> <li>• методы использования средств защиты информации при построении систем документооборота;</li> <li>• методы обеспечения юридической силы электронных данных;</li> <li>• основы действующего законодательства в области электронного документооборота</li> </ul> <p>Уметь:</p>
--	--	---

		<ul style="list-style-type: none"> <li>• оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>• навыками использовать основы правовых знаний в различных сферах деятельности</li> <li>• основной терминологией, методами и основными алгоритмами реализации защищенного электронного документооборота.</li> </ul> <p>Предусмотрены следующие виды контроля освоения дисциплины: текущий контроль успеваемости в форме контрольной работы, а также промежуточная аттестация в форме зачета с оценкой и экзамена.</p> <p>Общая трудоемкость дисциплины составляет 6 зачётных единиц.</p>
	<p><b>МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «Моделирование процессов и систем защиты информации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цели дисциплины: формирование у студентов достаточно полного представления о существующих методах, средствах, методологиях и технологиях моделирования процессов и систем защиты информации.</p> <p>Задачи дисциплины: ознакомить студентов с основными понятиями и подходами моделирования процессов и систем защиты информации; научить разрабатывать модели систем и процессов, проводить эксперименты на моделях, анализировать результаты моделирования.</p> <p>Дисциплина (модуль) направлена на формирование следующих компетенций:</p> <p>ОПК-7 (способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты);</p> <p>ПК-12 (способность принимать участие в проведении экспериментальных исследований системы защиты информации);</p> <p>ПСК-3.1 (способностью проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности,</p>

		<p>определения их источников и целей).  В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>1) Знать:</p> <ul style="list-style-type: none"> <li>- терминологию моделирования процессов и систем защиты информации;</li> <li>- основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей;</li> <li>- основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах.</li> <li>- методологии и средства структурного моделирования процессов и систем</li> </ul> <p>2) Уметь:</p> <ul style="list-style-type: none"> <li>- использовать нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах;</li> <li>- использовать принципы и методы моделирования процессов и систем защиты информации;</li> <li>- использовать методологии и средства моделирования процессов и систем, основные принципы и приемы построения моделей;</li> <li>- анализировать результаты процесса моделирования, формулировать предложения по оптимизации и улучшению функционирования моделируемой системы или процесса.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- терминологией моделирования процессов и систем защиты информации;</li> <li>- навыками использования правовых и нормативных требований к определению и моделированию угроз безопасности информации в информационных системах;</li> <li>- методологиями и средствами моделирования процессов и систем;</li> <li>- навыками анализа результатов процесса моделирования, формулирования предложений по оптимизации и улучшению функционирования моделируемой системы или процесса.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, дискуссии и доклада, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины (модуля) составляет 4 зачетные единицы.</p>
	АТТЕСТАЦИЯ ОБЪЕКТОВ	Дисциплина «Аттестация объектов»

	<p>ИНФОРМАТИЗАЦИИ</p>	<p>информатизации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утверждённых ФСТЭК России.</p> <p>Задачи: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации, изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-5 – способность использовать нормативные правовые акты в профессиональной деятельности;</li> <li>• ПК-5 – способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;</li> <li>• ПК-10 – способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;</li> <li>• ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</li> <li>• ПК-12 – способность принимать участие в проведении экспериментальных исследований системы защиты информации</li> <li>• ПК-15 – способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и</li> </ul>
--	-----------------------	---

		<p>нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать организацию аттестации объектов по требованиям безопасности информации; способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов; виды и формы информации, подверженной угро-зам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия; инструментальные средства и системы программирования для решения профессиональных задач; нормативные документы по проведению аттестации объектов информатизации по требованиям безопасности информации</p> <p>Уметь формировать комплекс мер по информационной безопасности с учётом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; проводить предварительный технико-экономического анализ и обоснования проектных решений по обеспечению информационной безопасности; оформить рабочую техническую документацию с учётом действующих нормативных и методических документов в области информационной безопасности; оформить заявку на проведение аттестации объектов информатизации.</p> <p>Владеть способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности; навыками составления необходимых документов при проведении аттестации объектов информатизации</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практических заданий, промежуточная аттестация в форме зачёта с оценкой.</p>
--	--	--

		<p>Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p>АКТУАЛЬНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ</p>	<p>Дисциплина «Актуальные тенденции в области защиты информации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки –№ 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: является ознакомление студентов с современными тенденциями в области защиты информации, новейшими подходами к построению подсистем информационной безопасности и актуальными изменениями в нормативно-методической базе в этой сфере.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>– рассмотрение следующих актуальных тенденций в области защиты информации: интегрированные решения по защите информации, управление безопасностью информации и событий (SIEM-системы);</li> <li>– управление учетными записями (IdAM-системы), унифицированный доступ к приложениям на примере Единой системы идентификации и аутентификации (ЕСИА),</li> <li>– обеспечение безопасного взаимодействия с внешними информационными системами на примере Системы межведомственного электронного взаимодействия (СМЭВ), тенденции в применении средств криптографической защиты информации (средств легковесной криптографии), в том числе в системах электронного документооборота, использование «облачных» технологий при реализации механизмов безопасности;</li> <li>– многоагентные системы в сфере информационной безопасности; безопасность Интернета вещей (Internet of Things, IoT).</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ПК-9 – способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;</li> <li>– ПК-14 – должен обладать способностью</li> </ul>

		<p>организовывать работу малого коллектива исполнителей в профессиональной деятельности. В результате освоения дисциплины обучающийся должен:</p> <p>Знать: перспективные направления развития информационной безопасности, наиболее актуальные решения в области криптографической, инженерно-технической и программно-аппаратной защиты информации, наиболее актуальные документы, создаваемые регуляторами в области информационной безопасности; особенности применения современных СЗИ для защиты персональных данных и информации, обрабатываемой в государственных информационных системах; методологические и технологические основы работы малого коллектива исполнителей.</p> <p>Уметь: ориентироваться на рынке современных средств защиты информации, выбирать оптимальное решение при проектировании и модернизации подсистемы информационной безопасности, выдвигать обоснованные предложения по применению таковых решений; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы.</p> <p>Владеть: навыками интеграции и эксплуатации наиболее актуальных средств защиты информации, использования современных средств криптографической защиты информации и систем контроля и управления доступом; навыками работы с системами защищенного документооборота; навыками работы с документацией.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практических заданий, промежуточная аттестация в форме экзамена.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.</p>
	<p><b>ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ</b></p>	<p>Дисциплина «История защиты информации» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Целью курса является овладение знаниями о закономерностях становления и тенденциях развития и совершенствования системы защиты информации, соотношении (связи) процессов прошлого и событий современности; формирование способности критически применять и переосмысливать накопленный</p>

		<p>исторический опыт, перерабатывать большие объемы информации и проводить целенаправленный поиск в различных источниках информации по профилю деятельности.</p> <p>Задачи: изучение состава защищаемой информации на различных этапах развития государства; классификацию защищаемой информации в различные исторические периоды по видам тайны, собственнику и др.; структуру угроз защищаемой информации в различные исторические периоды; каналы несанкционированного доступа к защищаемой информации и методов ее добывания в различные исторические периоды; особенности государственной политики в области защиты информации; процесс развития и совершенствования нормативной базы защиты информации; состав органов защиты информации в различные периоды развития системы защиты информации; направления и методы защиты информации; факторы, определяющие современную систему защиты информации и тенденции ее развития; современные направления научных исследований в области истории защиты информации; проблемное поле и современное состояние исследований по историографии защиты информации.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>– ОПК-4: способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li> <li>– ПК-10: способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды; основные направления государственной политики в области защиты; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты;</p>
--	--	---



		<p>Уметь применять полученные знания в научно-исследовательской и практической работе; формулировать научные проблемы и иметь навык в поиске методов их решения; историографически обосновывать собственную исследовательскую проблему; применять навыки методологических операций в научно-исследовательской деятельности;</p> <p>Владеть основными комплексами знания, которые включают в себя: понятия и термины, используемые и дискутируемые в различные исторические периоды становления и развития системы защиты информации, а также в современный период; основные исторические научные школы в области защиты информации и продукты их деятельности – научные концепции; главные труды крупнейших исследователей истории защиты информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, тестирования и реферата, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ</p>	<p>Дисциплина (модуль) «Системы защиты информации в зарубежных странах» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование знаний у обучающихся о закономерностях становления и тенденциях развития систем защиты информации в ведущих зарубежных странах, особенностях их современной организации и функционирования, перспективах развития и возможностях совершенствования зарубежного опыта в России.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- изучение процесса формирования и развития систем защиты информации в ведущих зарубежных странах;</li> <li>- анализ состава органов защиты информации и особенностей классификации защищаемой информации;</li> <li>- освоение современного опыта организации систем защиты информации в ведущих зарубежных странах.</li> </ul> <p>Дисциплина (модуль) направлена на</p>

		<p>формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-4 - способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li> <li>• ПК-10 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- основные направления государственной политики в области защиты информации в ведущих зарубежных странах;</li> <li>- состав, структуру и основные направления деятельности органов защиты информации в ведущих зарубежных странах.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- использовать зарубежный опыт при разработке комплексной системы защиты информации;</li> <li>- применять полученные знания в научно-исследовательской и практической работе.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- основными комплексами знаний о тенденциях и перспективах развития систем защиты информации в ведущих зарубежных странах;</li> <li>- навыками критически переосмысливать и применять накопленный зарубежный опыт в области информационной безопасности.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и контрольных работ, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ. ПРАКТИКУМ</p>	<p>Дисциплина (модуль) «Экономика защиты информации. Практикум» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование знаний у обучающихся об экономических методах защиты информации как части общих организационных мер, умений использовать современные методы расчетов для определения экономической целесообразности применения различных видов и средств защиты информации, что позволяет обеспечивать выбор наиболее</p>

		<p>эффективных проектов инвестиций в защиту информации.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- изучение вопросов, связанных с экономическими аспектами защиты информации, исследование стоимостных показателей информации и видов ущерба, наносимых информации;</li> <li>- выявление основных подходов к определению затрат на защиту информации, оценка эффективности применяемых методов защиты и системы защиты информации в целом.</li> </ul> <p>Дисциплина (модуль) направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- базовые экономические понятия и критерии определения эффективности хозяйственно-экономической деятельности;</li> <li>- основные положения определения экономической эффективности защиты информации и методы оценки эффективности инвестиций в защиту информации;</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- выбирать методы определения ущерба, наносимого владельцу информации в результате противоправного ее использования;</li> <li>- определять расчетным и экспертным методами стоимостные оценки ущерба;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- сведениями из нормативно-правовых документов по экономической составляющей систем защиты информации;</li> <li>- способностью осуществлять технико-экономическое сопровождение и обоснование проектных решений по обеспечению информационной безопасности.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и контрольной работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы .</p>
	<p><b>ОСНОВЫ КОНФИДЕНЦИАЛЬНОГО</b></p>	<p>Дисциплина «Основы конфиденциального делопроизводства» является вариативной частью</p>

ДЕЛОПРОИЗВОДСТВА	<p>блока дисциплин учебного плана, реализуется в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.</p> <p>Дисциплина «Основы конфиденциального делопроизводства» входит в вариативную часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».</p> <p>Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.</p> <p>Цель курса: формирование знаний у студентов по научным, прикладным и методическим аспектам организации выполнения технологических стадий, процедур и операций в процессе рассмотрения, исполнения и использования конфиденциальных документов в любых структурах государственной и негосударственной сфер, проектирование рациональной технологической схемы защищенного документооборота. При этом документооборот отражает весь "жизненный цикл" документа, включая его использование на стадии архивного хранения.</p> <p>Структура курса предполагает рассмотрение теоретических и практических аспектов в работе с конфиденциальными документами на предприятии, а также разбор на практических примерах ситуаций с конфиденциальным документооборотом.</p> <p>Дисциплина направлена на формирование следующих компетенций выпускника:</p> <p>ПК-8 - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</p> <p>ПК-9 - способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p>
------------------	---

		<p>Знать:</p> <ul style="list-style-type: none"> <li>-основы информационного права, сущность конфиденциальности информации и знать виды носителей информации и особенности фиксации на них информации;</li> <li>- основную научно-технической литературу, нормативные и методические документы в области обеспечения информационной безопасности</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</li> <li>- оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками использовать основы правовых знаний в различных сферах деятельности</li> <li>- навыками использовать основы правовых знаний в различных сферах деятельности</li> </ul> <p>Предусмотрены следующие виды контроля освоения дисциплины: текущий контроль успеваемости в форме контрольной работы, а также промежуточный аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы</p>
	<p><b>ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p>Дисциплина «Организация защита персональных данных» является вариативной частью блока дисциплин учебного плана, реализуется в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.</p> <p>Дисциплина «Организация защита персональных данных» входит в вариативную часть цикла по выбору студентов дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».</p> <p>Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.</p> <p>Содержание дисциплины охватывает круг вопросов, связанных с организацией обработки</p>

		<p>персональных данных, в соответствии с требованиями российского законодательства, применительно к различным категориям исполнителей на предприятии (от руководителей предприятий и структурных подразделений до непосредственно отвечающих за защиту информации и работающих с персональными данными). Анализируются изменения российского законодательства в части персональных данных, последствия внесения этих изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой персональных данных и затрат на их защиту.</p> <p>Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности персональных данных и используемых информационных технологий, способы снижения рисков утечки персональных данных.</p> <p>Структура курса предполагает рассмотрение теоретических и практических аспектов в работе с персональными данными на предприятии, а также разбор на практических примерах действий операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношениях, связанных с передачей и представлением персональных данных третьим лицам, в том числе органам государственной власти.</p> <p>Дисциплина направлена на формирование следующих компетенций выпускника:</p> <p>ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p> <p>ПК-10 - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p> <p>ПК-11 - способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</p> <p>ПК-12 - способностью принимать участие в проведении экспериментальных исследований системы защиты информации</p> <p>ПК-15 - способностью организовывать технологический процесс защиты информации</p>
--	--	--

		<p>ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю</p> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p><b>Знать:</b> базовые международные и российские регуляторы по информационной безопасности; сущность информации, методы и способы её отражения и передачи; случайные события и случайные величины, законы распределения; закон больших чисел, методы статистического анализа навыками по моделированию источников угроз и угроз безопасности объектов информатизации особенности практической деятельности всех перечисленных в Гражданском кодексе РФ юридических лиц, классифицируемых по основной цели деятельности, организационно-правовой форме и характеру прав, возникающих у их учредителей (участников) в связи с участием последних в образовании имущества учреждаемого ими юридического лица;</p> <p><b>Уметь:</b> работать со стандартами и нормативными документами; оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов вычислять вероятности случайных событий, составлять и исследовать функции распределения случайных величин, определять числовые характеристики случайных величин; обрабатывать статистическую информацию для оценки значений параметров и проверки значимости гипотез организовать работу по обеспечению безопасности объектов информатизации от воздействия источников угроз и угроз. осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм</p> <p><b>Владеть:</b> навыками использования международных и национальных стандартов в своей профессиональной деятельности навыками использовать основы правовых знаний в различных сферах деятельности вероятностным подходом к постановке и</p>
--	--	---

		<p>решению задач, навыками работы с библиотеками прикладных программ для решения вероятностных и статистических задач состава и порядка разработки нормативных документов по обеспечению безопасности объектов информатизации.</p> <p>способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю</p> <p>Предусмотрены следующие виды контроля освоения дисциплины: текущий контроль успеваемости в форме контрольной работы, тестирования, а также промежуточный аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>НЕЙРОННЫЕ СИСТЕМЫ</b></p>	<p>Дисциплина «НЕЙРОННЫЕ СИСТЕМЫ» Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме, реализуется на факультете информационных систем и безопасности ИИНТБ РГГУ, кафедрой информационных технологий и систем.</p> <p><u>Цель дисциплины:</u> изучение основных принципов организации информационных процессов в нейрокомпьютерных системах</p> <p><u>Задачи:</u></p> <ul style="list-style-type: none"> <li>• изучение методики синтеза нейронных сетей различной структуры;</li> <li>• исследование надежности и диагностики нейронных сетей;</li> <li>• изучение областей применения нейронных сетей: распознавание образов, принятие решений, кластеризация, прогнозирование, аппроксимация, сжатие данных;</li> <li>• изучение принципов построения нейрокомпьютеров;</li> <li>• формирование навыков разработки и реализации программных моделей нейронных сетей и нейрокомпьютерных систем.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ПК-12 – Способность принимать участие в проведении экспериментальных исследований системы защиты информации.</p> <p>В результате освоения дисциплины обучающийся должен:</p>



		<p>Знать:</p> <ul style="list-style-type: none"> <li>• основные принципы организации информационных процессов в нейροкомпьютерных системах;</li> <li>• основные архитектуры нейронных сетей, нейροкомпьютерных систем и области их применения;</li> <li>• основные способы и правила обучения нейροкомпьютерных систем .</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>• делать оценки и сравнивать качество обучения и функционирования различных моделей нейροкомпьютерных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>• навыками разработки и реализации программных моделей нейροкомпьютерных систем информации, постановки цели и выбора путей её достижения; навыками работы в коллективе, ответственности за поддержание партнерских, доверительных отношений.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практической работы, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ</p>	<p>Дисциплина «Управление информационными системами» является вариативной частью блока дисциплин учебного плана. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины: формирование знаний о процессах управления всеми средствами защиты информации и мониторинге безопасности информационной системы.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>-освоение знаний об архитектуре управления информационной безопасностью (ИБ) корпоративной информационной системы (КИС), функциональных системах управления и мониторинге безопасности КИС;</li> <li>-приобретение практических навыков по использованию соответствующих нормативно-правовых документов и программных инструментов для управления ИБ.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК - 7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры</li> </ul>

		<p>и содержания информационных процессов и особенностей функционирования объекта защиты;</p> <ul style="list-style-type: none"><li>• ПК – 15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации.</li></ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>знать:</p> <ul style="list-style-type: none"><li>• как формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой реализуемости и экономической целесообразности;</li><li>• как организовать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;</li><li>• как определить виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;</li></ul> <p>уметь:</p> <ul style="list-style-type: none"><li>• принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;</li><li>• собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;</li><li>• применять комплексный подход к обеспечению информационной безопасности ;</li></ul> <p>владеть:</p> <ul style="list-style-type: none"><li>• навыками работы с нормативными правовыми актами;</li><li>• навыками организации работы малого коллектива исполнителей с учетом требований защиты информации.</li></ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме выполнения практических заданий, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины</p>
--	--	--

	<p>БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</p>	<p>составляет 3 зачетных единицы.</p> <p>Дисциплина «Безопасность программного обеспечения» относится к вариативной части частью блока дисциплин учебного плана по направлению подготовки 10.03.01 «Информационная безопасность», профиля КЗОИ Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: приобретение знаний о базовых методах и способах защиты программного обеспечения автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа.</p> <p>Задачи: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищённом исполнении</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ПК-2 – способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p>ПК-15 – способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России</p> <p>В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:</p> <p>Знать:</p> <p>основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа;</p>
--	--	--

		<p>нормативные правовые документы в области защиты информации;</p> <p>математические модели безопасности и формальные модели доступа систем;</p> <p>модели и методы защиты операционных систем;</p> <p>принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств;</p> <p>основные проектные решения, средства и методы защиты информации от несанкционированного доступа.</p> <p>Уметь:</p> <p>решать типовые задачи с помощью методов защиты информации от несанкционированного доступа;</p> <p>применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия;</p> <p>выбирать, устанавливать и настраивать средства средства системного, прикладного и специального назначения;</p> <p>применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования.</p> <p>Владеть:</p> <p>методами разработки и использования средств защиты ПО;</p> <p>навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач;</p> <p>навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, реферата, тестирования, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p>ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ, УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ</p>	<p>Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная</p>

		<p>безопасность (профили подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: научить студентов приемам работы с инфраструктурой открытых ключей и цифровыми сертификатами.</p> <p>Задачи: формирование у студентов представлений об инфраструктуре открытых ключей, выработка умений разворачивать и настраивать удостоверяющие центры, научить студентов использовать механизмы обеспечения юридической значимости документов.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.</li> <li>• ПК-11 – должен обладать способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.</li> <li>• ПК-12 – способностью принимать участие в проведении экспериментальных исследований системы защиты информации.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать архитектуру и компоненты инфраструктуры открытых ключей, юридические и методические основы обеспечения юридической значимости электронных документов, принципы формирования электронной подписи, формат цифрового сертификата; методики, обработку, оценку погрешности и достоверности их результатов; профили тестирования, технология автоматизации тестов по оценке уровня защищенности.</p> <p>Уметь пользоваться основными криптопровайдерами в части формирования электронной подписи, разворачивать такие компоненты инфраструктуры как удостоверяющие центры, выбирать, устанавливать и настраивать компоненты инфраструктуры, принимать участие в разработке политики безопасности; проводить эксперименты и оценивать результаты тестирования; исследовать средства защиты информации, уметь оценивать по</p>
--	--	---

		<p>функциональным возможностям, надежности функционирования, эффективности обнаружения попыток НСД; исследовать средства защиты информации, уметь оценивать по функциональным возможностям, надежности функционирования, эффективности обнаружения попыток НСД.</p> <p>Владеть профессиональной терминологией, навыками настройки и эксплуатации компонентов инфраструктуры открытых ключей; навыками проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; навыками в проведении экспериментальных исследований системы защиты информации.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и лабораторных заданий, промежуточная аттестация в форме зачёта и курсовой работы.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.</p>
	<p><b>ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА</b></p>	<p>Дисциплина «Защита информации от несанкционированного доступа» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от НСД; формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.</p> <p>Задачи: овладение методами решения профессиональных задач по защите информации от НСД; формирование навыков работы с современными средствами защиты информации от НСД.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <p>ПК-11 - способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов</p> <p>ПК-12 - способность принимать участие в проведении экспериментальных исследований системы защиты информации</p> <p>ПК-15 - способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с</p>

		<p>нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные модели доступа (мандатная, дискреционная, ролевая и др.), принципы и методы защиты информации от НСД; принципы организации информационных систем в соответствии с требованиями по защите информации от НСД.</p> <p>Уметь формулировать и настраивать политику безопасности в информационной системе; осуществлять меры по защите информации от НСД, пользоваться нормативными документами по защите информации от НСД; анализировать и оценивать угрозы безопасности информационной системы.</p> <p>Владеть методикой анализа защищённости информационной системы; методами и средствами выявления угроз её информационной безопасности.</p> <p>По дисциплине предусмотрен текущий контроль в форме опросов и лабораторных работ, промежуточная аттестация в форме зачёта и защиты курсовой работы.</p> <p>Общая трудоёмкость освоения дисциплины составляет 4 зачётных единицы.</p>
	<p><b>БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ НА БАЗЕ TCP/IP</b></p>	<p>«Дисциплина «Безопасность информационных технологий и сетей на базе TCP/IP» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки –№ 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.»</p> <p>Цель дисциплины: приобретение знаний о базовых методах и способах защиты сетевых технологий и умений применять на практике средства защиты сетевых протоколов, в том числе стека протоколов TCP/IP.</p> <p>Задачи дисциплины: изучение принципов сетевого взаимодействия; выработка умений настраивать и применять средства сетевого взаимодействия, использовать инструменты настройки сетевой инфраструктуры, в том числе на базе стека протоколов TCP/IP.</p>

		<p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ОПК-7 – должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.</li> <li>• ПК-3 – должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты.</li> <li>• ПК-6 – должен обладать способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.</li> </ul> <p>В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:</p> <p>Знать:</p> <p>основные положения теории информационной безопасности и практики защиты информации в телекоммуникационных сетях;  модели угроз безопасности информации;  структуру и содержание информационных процессов и особенностей функционирования объекта защиты на базе TCP/IP;  основные сервисы и механизмы шифрования и аутентификации информации по модели OSI/ISO;  модели и методы защиты сетей на базе TCP/IP;  нормативные правовые документы в области защиты информации;</p> <p>Уметь:</p> <p>осуществлять базовые настройки сетевых устройств 2-го и 3-го уровня согласно модели OSI/ISO;  обнаруживать ошибки в настройках маршрутизации;  решать типовые задачи администрирования систем защиты информации;  применять современные методы и методики защиты сетевых технологий;  организовывать мероприятия по аттестации объекта информатизации по требованиям безопасности информации.</p> <p>Владеть:</p> <p>навыками настройки и эксплуатации коммуникационного оборудования.  методами использования средств защиты</p>
--	--	--



		<p>протоколов стека TCP/IP;  навыками эксплуатации защищенных протоколов стека TCP/IP.  навыками организации и сопровождении процесса аттестации объекта информатизации по требованиям безопасности информации.  Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, реферата, тестирования, промежуточная аттестация в форме зачета с оценкой.  Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.</p>
	<p><b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  МОБИЛЬНЫХ УСТРОЙСТВ</b></p>	<p>Дисциплина «Информационная безопасность мобильных устройств» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере мобильных систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;</li> <li>– сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;</li> <li>– сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>- ОПК-4 – способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;</li> <li>- ПСК3.3 - способностью участвовать в</li> </ul>

		<p>реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты;</p> <p>- ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: технологию определения состава защищаемых информационных ресурсов.</p> <p>Уметь: настраивать и эксплуатировать мобильные системы</p> <p>Владеть: методами и инструментами анализа защищенности объектов информатизации с помощью мобильных систем.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических занятий, промежуточная аттестация в форме зачета с оценкой.</p> <p>Общая трудоёмкость освоения дисциплины составляет 3 зачётных единицы.</p>
	<p>СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (DLP-СИСТЕМЫ)</p>	<p>Дисциплина «Системы защиты от утечки конфиденциальной информации (DLP-системы)» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации.</p> <p>Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере DLP-систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>– сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;</li> <li>– сформировать представления об уязвимостях, присущих объектам информатизации, связанных</li> </ul>

		<p>с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;</p> <p>– сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>- ОПК-7 - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</li> <li>- ПК-13 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ;</li> <li>- ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: технологию определения состава защищаемых информационных ресурсов.</p> <p>Уметь: настраивать и эксплуатировать DLP-системы</p> <p>Владеть: методами и инструментами анализа защищенности объектов информатизации с помощью DLP-систем.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме практических заданий, промежуточная аттестация в форме зачета.</p> <p>Общая трудоёмкость освоения дисциплины составляет 2 зачётных единицы.</p>
	<p>ОРГАНИЗАЦИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ</p>	<p>Дисциплина «Организация виртуальных частных сетей» является вариативной частью блока дисциплин учебного плана, реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль</p>

		<p>подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.</p> <p>Цель дисциплины: формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по применению виртуальных частных сетей, оптимального выбора и интеграции сетевых протоколов виртуальных частных сетей (ВЧС).</p> <p>Задачи: рассмотрение существа проблемы безопасной передачи информации в информационных системах, основных способов обеспечения конфиденциальности и целостности информации при её передаче, основных протоколов, применяемых для организации защищённых ВЧС, критериев выбора оптимальных схемных решений для организации защищённых ВЧС на канальном, сетевом и прикладном уровнях.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"> <li>• ПК-13 – способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.</li> </ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать основные виды угроз безопасности информации при её передаче по компьютерным сетям; способы построения виртуальных каналов; протоколы организации ВЧС.</p> <p>Уметь проводить анализ проблем безопасности передачи информации с точки зрения конфиденциальности и целостности; проводить анализ и выбор сетевых протоколов ВЧС.</p> <p>Владеть приёмами настройки и применения современных сетевых протоколов ВЧС.</p> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и практического задания, промежуточная аттестация в форме зачёта.</p> <p>Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.</p>
	<p>ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ</p>	<p>Дисциплина является вариативной частью блока дисциплин учебного плана. Реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационных технологий и систем.</p> <p>Содержание дисциплины охватывает круг</p>

		<p>вопросов, связанных с организацией сбора, обработки и хранения информации, а также разработкой и эксплуатацией информационных ресурсов и систем, средств обеспечения автоматизированных информационных систем и их технологий, используемых в профессиональной деятельности.</p> <p>Цель дисциплины - повышение общей информационной культуры на основе освоения понятийного аппарата информатики и ИКТ, формирование профессиональных компетенций выпускника, который знает возможности современных компьютеров, и аппаратные, программные средства для людей с ограниченными возможностями и инвалидов, владеет методами сбора, хранения и обработки данных в информационных системах, используемых при подготовке решений в профессиональной деятельности людей с ограниченными возможностями здоровья и инвалидов.</p> <p>Задачи: формирование знания, навыков и умений работы с современными компьютерными и программными средствами, включая аппаратные и программные средства для лиц с ограниченными возможностями, при решении прикладных задач в профессиональной деятельности.</p> <p>Дисциплина направлена на формирование следующих компетенций:</p> <ul style="list-style-type: none"><li>• ОК-8 способностью к самоорганизации и самообразованию</li></ul> <p>В результате освоения дисциплины обучающийся должен:</p> <p><u>Знать</u>: способы применения информационно-коммуникационных технологий в различных направлениях профессиональной деятельности; назначение и виды информационно-коммуникационных технологий, применяемых для формирования требований к информационной системе предприятия, работающих с лицами с ОВЗ. Инструментарий создания презентаций. Правила создания презентаций; методологию, модели, методы и способы создания информационных систем для лиц с ОВЗ.</p> <p><u>Уметь</u>: формулировать и осуществлять постановку задач при разработке презентации программного продукта.</p> <p><u>Владеть</u>: базовыми современными ИКТ в различных направлениях профессиональной деятельности; международными и</p>
--	--	--

		<p>отечественными стандартами в области информационных систем и технологий для разработки и оптимизации информационных систем, поддерживающих работу лицами с ОВЗ. Навыками и средствами разработки презентаций. Навыками эксплуатации специализированного программного обеспечения.</p> <p>По дисциплине предусмотрен текущий контроль в форме самостоятельной работы и доклада, промежуточная аттестация в форме зачёта.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p>АДАПТАЦИЯ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ</p> <p>К</p>	<p>Дисциплина «Адаптация к профессиональной деятельности является базовой частью блока дисциплин учебного плана. Реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой психологии семьи и детства.</p> <p>Цель дисциплины: ознакомление студентов с системой социальных, медицинских и психолого-педагогических мероприятий, направленных на оказание помощи молодому человеку в профессиональном образовании с учетом его возможностей, склонностей, интересов, состояния здоровья, а также с учетом образовательной среды университета.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>самоанализ образовательных потребностей студентов, возможных трудностей при получении высшего профессионального образования;</li> <li>определение содержания и структуры профессионально-важных качеств в выбранной профессиональной сфере; самооценка выделенных студентами профессионально-важных качеств и компетенций; постановка задач на ближайшую и отдаленную перспективу овладения общекультурными и профессиональными компетенциями;</li> <li>ознакомление с гражданским, трудовым законодательством, с семейным правом, основными правовыми гарантиями в области социальной защиты, образования и труда инвалидов;</li> <li>обучение навыкам составления резюме, умениям использовать ИКТ в самообразовании и подготовке к занятиям;</li> <li>развитие навыков саморегуляции.</li> </ul> <p>Дисциплина направлена на формирование следующих компетенций:</p>

		<p>– ОК-6: способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;</p> <p>– ОК-8: способен к самоорганизации и самообразованию.</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- классификации профессий, трудности и типичные ошибки при выборе профессии;</li> <li>- основополагающие международные документы, относящиеся к правам инвалидов;</li> <li>- основы гражданского и семейного законодательства;</li> <li>- основы трудового законодательства, особенности регулирования труда инвалидов;</li> <li>- основные правовые гарантии инвалидам в области социальной защиты и образования;</li> <li>- современное состояние рынка труда, классификацию профессий и предъявляемых профессией требований к психологическим особенностям человека, его здоровью;</li> <li>- функции органов труда и занятости населения.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- использовать свои права адекватно законодательству;</li> <li>- обращаться в надлежащие органы за квалифицированной помощью;</li> <li>- анализировать и осознанно применять нормы закона с точки зрения конкретных условий их реализации;</li> <li>- составлять необходимые заявительные документы;</li> <li>- составлять резюме, осуществлять самопрезентацию при трудоустройстве;</li> <li>- использовать приобретенные знания и умения в различных жизненных и профессиональных ситуациях;</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- простейшими способами и приемами управления собственными психическими состояниями;</li> <li>- способами поиска необходимой информации для эффективной организации учебной и будущей профессиональной деятельности.</li> </ul> <p>По дисциплине предусмотрен текущий контроль в форме опроса и контрольных работ, промежуточная аттестация в форме зачёта.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	МИРОВЫЕ ИНФОРМАЦИОННЫЕ	Дисциплина «Мировые информационные ресурсы» является вариативной частью блока

РЕСУРСЫ	<p>дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цель дисциплины (модуля): формирование у обучающихся знаний о современных мировых и российских информационных ресурсах, их структуре, основных зарубежных и российских производителях информации, деловых и других ресурсах сети Интернет.</p> <p>Задачи дисциплины:</p> <ul style="list-style-type: none"> <li>- раскрыть структуру и содержание современных мировых и российских информационных ресурсов;</li> <li>- ознакомить студентов с состоянием российского и мирового рынка информации и предоставляемыми им услугами;</li> <li>- способствовать освоению обучающимися основных технологий доступа к информационным ресурсам и ресурсам знаний.</li> </ul> <p>Дисциплина (модуль) направлена на формирование следующей компетенции:</p> <ul style="list-style-type: none"> <li>• ПК-10 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.</li> </ul> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> <li>- требования к составу и содержанию информации при решении практических задач;</li> <li>- общее состояние мировых информационных ресурсов (поставщики информации, виды информационных услуг, технологии доступа к информации);</li> <li>- основные информационные ресурсы Интернета, виды предоставляемых услуг;</li> <li>- основных зарубежных и российских производителей профессиональной информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- определять информационные потребности для решения конкретной задачи;</li> <li>- получать доступ к информационным ресурсам;</li> <li>- давать профессиональную оценку полученной информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками определения информационных потребностей для решения конкретной задачи и получения доступа к мировым информационным ресурсам;</li> </ul>
---------	---



		<ul style="list-style-type: none"> <li>- навыками профессиональной оценки полученной информации;</li> <li>- навыками использования найденной в мировых ресурсах информации при решении практических задач.</li> </ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса и контрольных работ, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
	<p><b>НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ</b></p>	<p>Дисциплина «Надежность информационных систем» является вариативной частью блока дисциплин учебного плана, реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.</p> <p>Цели дисциплины (модуля): формирование у студентов теоретических знаний о принципах построения, составе, назначении, характеристиках и особенностях применения технических средств и систем с точки зрения надежности, необходимых умений и практических навыков в области анализа информационных систем с заданным уровнем надежности.</p> <p>Задачи:</p> <ul style="list-style-type: none"> <li>- освоение студентами методического подхода для проведения анализа надежности информационных систем;</li> <li>- изучение законов распределения теории надежности;</li> <li>- изучение структуры и состава систем диагностики, навыков их выбора и разработки.</li> </ul> <p>Дисциплина (модуль) направлена на формирование следующих компетенций:</p> <p>ПК-10 (способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности).</p> <p>В результате освоения дисциплины (модуля) обучающийся должен:</p> <p>1) Знать:</p> <ul style="list-style-type: none"> <li>- функциональные и числовые показатели надежности и ремонтпригодности технических и программных элементов и систем;</li> <li>- методы анализа (расчета) надежности информационных систем;</li> <li>- способы анализа технической эффективности информационных систем;</li> <li>- современные методы выбора с точки зрения</li> </ul>

		<p>надежности технических и программных средств автоматизации для построения информационных систем;</p> <p>2) Уметь:</p> <ul style="list-style-type: none"><li>- определять по результатам испытаний и наблюдений оценки показателей надежности и ремонтпригодности технических элементов и систем;</li><li>- анализировать надежность информационных систем;</li></ul> <p>3) Владеть:</p> <ul style="list-style-type: none"><li>- навыками анализа (расчета) надежности информационных систем;</li><li>- навыками определения по результатам испытаний и наблюдений оценок показателей надежности и ремонтпригодности технических элементов и систем.</li></ul> <p>Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, дискуссии и доклада, промежуточная аттестация в форме зачета.</p> <p>Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.</p>
--	--	--