

**Аннотации рабочих программ дисциплин (модулей) образовательной программы по направлению подготовки 10.04.01 «Информационная безопасность», направленность подготовки «Безопасность информационного и программного обеспечения автоматизированных систем»**

<b>Название:</b>		Б1.Б.1. Защищенные информационные системы
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОК-2; ПК-4; ПК-7
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;</li> <li>– основные методы и средства обеспечения безопасности операционных систем;</li> <li>– основные методы и средства обеспечения сетевой безопасности;</li> <li>– основные методы и средства обеспечения безопасности в системах управления базами данных;</li> </ul>
	<b>уметь:</b>	осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;
	<b>владеть навыками /иметь опыт:</b>	настройки подсистем защиты основных операционных систем.
<b>Содержание:</b>		<p>Защита в операционных системах. Механизмы защиты операционной системы</p> <p>Интеграция защищенных операционных систем. Типовые угрозы сетевой безопасности. Методы и средства обеспечения информационной безопасности в вычислительных сетях.</p> <p>Защита в системах управления базами данных. Теоретические основы безопасности в СУБД</p>
<b>Форма промежуточной аттестации:</b>		<p>Экзамен</p> <p>Курсовой проект</p>

<b>Название:</b>		Б1.Б.2. Технология обеспечения информационной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):</b>		ОК-2; ПК-2, ПК-14
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– место и роль информационной безопасности в системе национальной безопасности Российской Федерации;</li> <li>– методы концептуального проектирования технологий обеспечения информационной безопасности;</li> <li>– принципы построения информационных систем;</li> <li>– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;</li> <li>– принципы организации информационных систем в соответствии с требованиями по защите информации.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;</li> <li>– осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.</li> <li>– анализировать и оценивать угрозы информационной безопасности объекта;</li> <li>– осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;</li> <li>– обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;</li> <li>– организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– навыками выявления и уничтожения компьютерных вирусов;</li> <li>– методами и средствами выявления угроз безопасности автоматизированным системам;</li> <li>– методами анализа и формализации информационных процессов объекта и связей между ними;</li> <li>– пользования профессиональной терминологией.</li> </ul>
<b>Содержание:</b>		<p>Обзор персонального компьютера. Безопасные лабораторные процедуры и использование инструментов. Сборка компьютера – пошаговые инструкции. Основы профилактического обслуживания и устранения неисправностей. Сведения об операционных системах. Сведения о портативных ПК и других устройствах. Сведения о принтерах и сканерах. Основные сведения о сетях. Дополнительные сведения о персональных компьютерах и сетях. Основы безопасности. Коммуникационные навыки. Дополнительные сведения о</p>

	безопасности.
<b>Форма промежуточной аттестации:</b>	Зачет

<b>Название:</b>		Б1.Б.3. Управление информационной безопасностью
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОК-1; ОПК-2; ПК-13; ПК-15
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	методы и средства управления информационной безопасностью;
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– проводить общую самооценку соответствия организации требованиям нормативных документов и Стандартам по информационной безопасности;</li> <li>– выявлять и анализировать характеристики возможных угроз и каналов утечки информации;</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– навыками управления информационной безопасностью простых объектов</li> <li>– работы с нормативной документацией по обеспечению информационной безопасности;</li> <li>– работы с программно-аппаратными средствами обеспечения информационной безопасности</li> </ul>
<b>Содержание:</b>		<p>Структура документа. Ключевые средства контроля. Задание требований к информационной безопасности организации. Оценка рисков нарушения безопасности. Факторы, необходимые для успеха. Разработка собственных рекомендаций Общие положения. Назначение. Информативные ссылки. Термины и определения. Политика безопасности. Политика информационной безопасности Организация защиты Инфраструктура информационной безопасности. Безопасность доступа сторонних организаций. Идентификация рисков, связанных с подключениями сторонних организаций. Условия безопасности в контрактах, заключённых со сторонними организациями Классификация ресурсов и их контроль. Ответственность за ресурсы. Классификация информации Безопасность персонала.</p> <p>Безопасность в должностных инструкциях и при выделении ресурсов. Обучение пользователей Реагирование на события, таящие угрозу безопасности Физическая безопасность и безопасность окружающей среды. Защищённые области. Защита оборудования. Администрирование компьютерных систем и вычислительных сетей. Операционные процедуры и обязанности. Планирование систем и их приёмка. Защита от вредоносного программного обеспечения. Обслуживание систем. Сетевое администрирование.</p> <p>Оперирование с носителями информации и их защита. Обмен данными и программами Управление доступом к системам. Производственные требования к управлению доступом к системам. Управление доступом пользователей. Обязанности пользователей Управление доступом к сети. Управление доступом к компьютерам. Управление доступом к приложениям.</p> <p>Слежение за доступом к системам и их использованием Разработка и сопровождение информационных систем. Требования к</p>

	<p>безопасности систем Безопасность в прикладных системах. Защита файлов прикладных систем. Безопасность в среде разработки и рабочей среде Планирование бесперебойной работы организации. Вопросы бесперебойной работы организации. Выполнение требований. Выполнение правовых требований. Проверка безопасности информационных систем. Аудит систем.</p>
<p><b>Форма промежуточной аттестации:</b></p>	<p>Экзамен Курсовая работа</p>

<b>Название:</b>		Б1.Б.4. Информационные технологии в науке и производстве
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОК-2; ОПК-1; ПК-1
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	основные понятия теории игр основные разделы исследования операций (ИО) и решаемые в них задачи, методику проведения исследования операций, методы отыскания оптимальных решений в разных классах задач ИО
	<b>уметь:</b>	строить математическую модель задачи, подбирать метод ее решения, находить оптимальное решение и делать содержательную интерпретацию.
	<b>владеть навыками /иметь опыт:</b>	пользования терминологией исследования операций и соответствующим математическим аппаратом.
<b>Содержание:</b>		Общие вопросы ИО. Календарное планирование программ сетевыми методами. Теория игр. Теория массового обслуживания. Имитационное моделирование
<b>Форма промежуточной аттестации:</b>		Зачет

<b>Название:</b>		Б1.Б.5. Экономика и управление
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОК-2, ПК-1, ПК-16
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основные теории и методы макро- и микроэкономики</li> <li>– экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности);</li> <li>– современные формы и методы хозяйствования, нормативные правовые акты, регламентирующие деятельность предприятия;</li> <li>– социально-экономический и административно-хозяйственный механизм производственного процесса и понимать сущность деятельности предприятия;</li> <li>– основные экономические показатели деятельности предприятий и показатели оценки;</li> <li>– эффективности использования ресурсов предприятия.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности;</li> <li>– рассчитывать показатели эффективности использования производственных ресурсов предприятия;</li> <li>– анализировать и оценивать экономические показатели деятельности предприятия и влияние на них принимаемых менеджерами решений.</li> </ul>
	<b>Владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям;</li> <li>– практическими навыками решения конкретных технико-экономических и управленческих вопросов в области автоматизации технологических процессов и производств;</li> <li>– находить организационно - управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность</li> </ul>
<b>Содержание:</b>		<ol style="list-style-type: none"> <li>1. Предприятие как субъект и объект предпринимательской деятельности.</li> <li>2. Прибыль предприятия.</li> <li>3. Налогообложение предприятий</li> <li>4. Производственные ресурсы предприятия. Основной капитал</li> <li>5. Производственные ресурсы предприятия.оборотный капитал</li> <li>6. Производственные ресурсы предприятия. Трудовые ресурсы</li> <li>7. Издержки производства и себестоимость продукции предприятия.</li> <li>8. Эффективность хозяйственной деятельности.</li> <li>9. Функции и методы управления производством</li> <li>10. Процесс принятия управленческих решений и ответственность менеджеров всех уровней</li> </ol>
<b>Форма промежуточной аттестации:</b>		Экзамен

<b>Название:</b>		Б1.В.ОД.1. Философия и методология научного исследования
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-5, ПК-6, ПК-8
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>- основные методологические принципы научного исследования;</li> <li>- методы научного исследования;</li> <li>- структуру и содержание этапов исследовательского процесса;</li> <li>- методические требования к структуре и содержанию научного исследования;</li> <li>- правила и требования к оформлению диссертации.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>- квалифицированно ориентироваться в методологическом обеспечении исследования на философском, общенаучном, частно-научном и методическом уровнях познания;</li> <li>- формулировать решаемую проблему, определять объект и предмет исследования, ставить исследовательские задачи и разрабатывать план их решения;</li> <li>- разрабатывать программу исследования;</li> <li>- формулировать структуру и содержание этапов исследовательского процесса;</li> <li>- выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования.</li> <li>- формулировать и решать задачи, возникающие в ходе научно-исследовательской деятельности;</li> <li>- осуществлять поиск информации, необходимой для написания научной работы;</li> <li>- оформлять и представлять результаты проведённой исследовательской работы.</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>- использования достижений и основных понятий теории методологии науки для проведения самостоятельных научных исследований;</li> <li>- владеть приёмами постановки целей и задач научных и проектных исследований;</li> <li>- самостоятельной работы с литературой для поиска информации;</li> <li>- оформления и представления результатов проведённой исследовательской работы.</li> </ul>
<b>Содержание:</b>		<p>Понятие, сущность, виды научного исследования.  Научное исследование как творческий процесс.  Философские проблемы научного исследования.  Методологические основы научного исследования.  Методы эмпирического исследования.  Общелогические методы научного исследования.  Теоретические методы научного исследования.  Системность и синергетика – новые парадигмы методологии науки.  Этапы научного исследования.</p>



	Сбор научной информации. Основные источники информации. Оформление научных исследований. Методология диссертационного исследования
<b>Форма промежуточной аттестации:</b>	Экзамен

<b>Название:</b>		Б1.В.ОД.2. Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-3, ПК-14, ПК-16
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– законодательства об обеспечении безопасности государства, содержание основных понятий по правовому обеспечению безопасности государства;</li> <li>– правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;</li> <li>– понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;</li> <li>– основы правового регулирования взаимоотношений государства и граждан в области обеспечения безопасности государства.</li> </ul>
	<b>уметь:</b>	– отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– применять действующую законодательную базу в области информационной безопасности;</li> <li>– разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов, иметь навыки работы с нормативно-правовыми актами.</li> </ul>
<b>Содержание:</b>		<p>Правовой аспект проблемы общей теории безопасности РФ. Информационное противоборство как новый вид межгосударственной борьбы.</p> <p>Общий состав мер по обеспечению безопасности государства.</p> <p>Ограничение прав и свобод человека при обеспечении безопасности государства.</p> <p>Методологические основы и понятийный аппарат общей теории безопасности государства. Место общей теории безопасности государства в системе научных знаний.</p> <p>Основные понятия общей теории безопасности государства</p> <p>Система правового обеспечения общей теории безопасности РФ. Основные источники угроз национальной безопасности РФ.</p> <p>Международно-правовые основы деятельности государств по обеспечению безопасности. Ответственность за нарушение законодательства в сфере обеспечения безопасности государства. Государственная тайна и ее правовой статус.</p>
<b>Форма промежуточной аттестации:</b>		Экзамен

<b>Название:</b>		Б1.В.ОД.3. Методы и средства защиты информации в системах электронного документооборота
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-8, ПК-16
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основные понятия и принципы делопроизводства и электронного документооборота;</li> <li>– принципы функционирования автоматизированных систем поддержки документооборота и обеспечения их безопасности;</li> <li>– особенности сертификации и аттестации систем электронного документооборота по требованиям безопасности;</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– классифицировать и оценивать угрозы информационной безопасности для систем электронного документооборота;</li> <li>– разрабатывать модели угроз и модели нарушителя безопасности систем электронного документооборота;</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в системах электронного документооборота;</li> <li>– пользования методами и средствами выявления угроз безопасности системам электронного документооборота.</li> </ul>
<b>Содержание:</b>		Основные принципы и особенности организации электронного документооборота. Технологии обработки поступивших документов. Контроль исполнения документов. Порядок проверки наличия документов. Формирование и хранение конфиденциальных дел. Обеспечение безопасности документооборота.
<b>Форма промежуточной аттестации:</b>		Экзамен

<b>Название:</b>		Б1.В.ОД.4. Проектирование технических средств и систем в защищенном исполнении
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):</b>		ПК-2, ПК-3, ПК-7
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>- основные понятия, используемые при обеспечении информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении;</li> <li>- взаимосвязь обеспечения информационной безопасности с технологиями проектирования и создания (модернизации) объектов информатизации;</li> <li>- средства видов обеспечений компьютерной системы, подлежащие разработке при проектировании, создании (модернизации) компьютерной системы;</li> <li>- основные мероприятия по организации разработке средств видов обеспечения компьютерной системы, отвечающих требованиям информационной безопасности;</li> <li>- общие требования к технологической безопасности средств программного и информационного обеспечений компьютерных систем;</li> <li>- структуру и содержание программы обеспечения информационной безопасности проектирования, создания (модернизации) компьютерных систем в составе объектов информатизации;</li> <li>- требования к разработке средств основных видов обеспечения компьютерной системы в защищенном исполнении;</li> <li>- требования по обеспечению информационной безопасности стенда для разработки средств программного и информационного обеспечения;</li> <li>- требования информационной безопасности к документации на объекты информатизации на базе компьютерных систем;</li> <li>- структуру, цели создания, назначение и основные функции системы обеспечения информационной безопасности проектирования, создания (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении;</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>- определять основные мероприятия по организации разработки средств видов обеспечения компьютерной системы;</li> <li>- разработать требования к технологической безопасности средств программного и информационного обеспечения;</li> <li>- разрабатывать структуру и отдельные разделы программы обеспечения информационной безопасности проектирования, создания (модернизации) компьютерной системы в защищенном исполнении в составе объекта информатизации;</li> <li>- разрабатывать документы, регламентирующие обеспечение информационной безопасности разработки объектов</li> </ul>

		информатизации на базе компьютерных систем в защищенном исполнении;
	<b>владеть навыками /иметь опыт:</b>	работы с нормативными правовыми документами в области информационной безопасности; -разработки (формирования) требований информационной безопасности к объектам и субъектам деятельности по проектированию, созданию (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении;
	<b>Содержание:</b>	Введение в обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. Проектирование, создание, модернизация объектов информатизации на базе компьютерной системы в защищенном исполнении как объект обеспечения информационной безопасности. Проектирование, создание, модернизация объектов информатизации на базе компьютерной системы в защищенном исполнении как объект обеспечения информационной безопасности. Требования к документации на объект информатизации на базе компьютерной системы в защищенном исполнении и на его составные части, выполнение которых обеспечивает информационную безопасность разработки этих объектов и их составных частей. Система обеспечения информационной безопасности разработки ОИ на базе компьютерной системы в защищенном исполнении.
	<b>Форма промежуточной аттестации:</b>	Экзамен Курсовой проект

<b>Название:</b>		Б1.В.ОД.5. Теоретические основы управления
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-2, ПК-12, ПК-13
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	методы анализа, синтеза, способы математического моделирования и основные подходы к организации современных систем управления; особенности цифровых систем управления.
	<b>уметь:</b>	моделировать и выполнять необходимые операции с передаточными функциями; выполнять преобразования структурных схем систем управления, исследовать их переходные процессы и частотные характеристики; выполнять анализ динамики разомкнутых и замкнутых систем управления; применять цифровые системы управления для решения различных производственных задач; использовать микропроцессоры и микро-ЭВМ в системах управления; программно реализовывать алгоритмы управления в цифровых системах управления.
	<b>владеть навыками /иметь опыт:</b>	методами и программными средствами исследования и анализа устойчивости, управляемости и наблюдаемости систем управления; методами анализа технического уровня и эффективности средств и систем управления процессов пищевых, химических и других производств для обеспечения их соответствия обусловленным производственным условиям и экономическим показателям; способами поиска и применения для практических разработок материалов периодических, реферативных и справочно-информационных изданий по профилю организации эффективного управления процессами различных производств
<b>Содержание:</b>		Управление и информатика, общие принципы системной организации. Математические модели объектов и систем управления, формы представления моделей. Устойчивость, управляемость, наблюдаемость, инвариантность и чувствительность систем управления. Методы анализа и синтеза систем управления. Цифровые системы управления и их математическое описание. Использование микропроцессоров и микро-ЭВМ в системах управления. Анализ и синтез цифровых систем управления.
<b>Форма промежуточной аттестации:</b>		Зачет с оценкой

<b>Название:</b>		Б1.В.ОД.6. Информационно-аналитические системы безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-1, ПК-6, ПК-8
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	характеристики современного информационного общества, проблем защиты информации и обеспечения информационной безопасности;
	<b>уметь:</b>	– формировать представления о содержании аналитической работы по подготовке принятия управленческих решений; – анализировать технологии проектирования экспертных систем, а также систем, основанных на знаниях, с использованием соответствующих инструментальных средств;
	<b>владеть навыками /иметь опыт:</b>	– написания информационных обзоров и аналитических справок, а также разработки проектов; – участия и организации информационно-аналитической работы – разработки информационных хранилищ, экспертных систем, а также систем, основанных на знаниях, и администрирования информационно-аналитических и интеллектуальных систем.
<b>Содержание:</b>		1. Базовые понятия информационно-аналитических систем. 2. Информационное пространство как среда анализа и функционирования искусственного интеллекта. 3. Технологии сбора, хранения и оперативного анализа данных – концепция информационных хранилищ. 4. Технологии интеллектуального анализа данных. 5. Характеристика систем искусственного интеллекта. 6. Основы управления информационно-аналитическими и интеллектуальными системами и их проектирования.
<b>Форма промежуточной аттестации:</b>		Экзамен

<b>Название:</b>		Б1.В.ОД.7. Иностраннный язык в профессиональной сфере
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОПК-1, ПК-6
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– особенности иноязычного общения в типичных ситуациях, связанных с деловой поездкой за рубеж;</li> <li>– нормы невербального делового общения;</li> <li>– структуру фирмы/компании, названия должностей персонала;</li> <li>– структуру CV, резюме, договора.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– вести диалоги этикетного характера, используя вербальные и невербальные средства вежливого поведения на ИЯ;</li> <li>– использовать свой речевой аппарат общения коммуникативно приемлемо и правильно в ситуациях социально-культурного и делового общения при: <ul style="list-style-type: none"> <li>– знакомстве, представлении, личной встрече или разговоре по телефону с партнером по бизнесу, представлении другого лица;</li> <li>– подготовке к служебной поездке за рубеж (заказ авиабилета, онирование номера в гостинице);</li> <li>– прибытии в страну делового партнера (таможенный контроль, у администратора в гостинице, ориентация по городу, заказ блюд в ресторане и т.п.);</li> <li>– представлении фирмы/продукции/услуг;</li> <li>– подписании договора о поставках, сотрудничестве;</li> <li>– ориентироваться в структуре делового письма и извлекать основную информацию из текста деловой корреспонденции;</li> <li>– написать CV, резюме, деловое письмо с соблюдением общепринятых норм.</li> </ul> </li> </ul>
	<b>владеть навыками /иметь опыт:</b>	– Владеть лексическим минимумом и набором речевых клише для участия в обсуждении темы/проблемы по материалам прочитанных текстов, для аргументирования своей позиции (отношение к прочитанной информации), а также для общения с зарубежным партнером (телефонный разговор, факс, простое деловое письмо).
<b>Содержание:</b>		Предприятие (фирма, компания) по избранному направлению/профилю специалиста; Конечный продукт (услуги) производственной деятельности предприятия, фирмы; Проблемы сбыта продукции/оказания услуг в условиях современного рынка; Установление личного контакта с зарубежными партнерами по избранному направлению/профилю специалиста; Подготовка к итоговому контролю.
<b>Форма промежуточной аттестации:</b>		Экзамен



<b>Название:</b>		Б1.В.ОД.8. Теоретические основы компьютерной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-2, ПК-4, ПК-7
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– методологические и технологические основы комплексного обеспечения безопасности АС,</li> <li>– угрозы и методы нарушения безопасности АС,</li> <li>– формальные модели, лежащие в основе систем защиты АС,</li> <li>– стандарты по оценке защищенности АС и их теоретические основы,</li> <li>– методы и средства реализации защищенных АС,</li> <li>– методы и средства верификации и анализа надежности защищенных АС;</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– проводить анализ АС с точки зрения обеспечения компьютерной безопасности,</li> <li>– разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы,</li> <li>– применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС,</li> <li>– реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– работы с АС распределенных вычислений и обработки информации;</li> <li>– работы с документацией АС,</li> <li>– использования критериев оценки защищенности АС,</li> <li>– построения формальных моделей систем защиты информации АС.</li> </ul>
<b>Содержание:</b>		<p>Основные понятия теории компьютерной информации. Архитектура электронных систем обработки данных.</p> <p>Модели безопасности. Анализ угроз информационной безопасности. Анализ причин нарушений безопасности. Изъяны защиты. Структура теории безопасности. Уровни защиты информации.</p> <p>Построение систем защиты от угрозы нарушения конфиденциальности информации. Особенности применения криптографических методов защиты информации. Способы реализации криптографической подсистемы. Построение систем защиты от угрозы нарушения целостности информации.</p> <p>Особенности реализации систем с симметричными и несимметричными ключами. Цифровая подпись.</p> <p>Построение систем защиты от угрозы раскрытия параметров информационной системы. Методология построения защищенных систем. Политика безопасности. Методы построения защищенных автоматизированных систем. Формальные модели безопасности.</p> <p>Модель матрицы доступов HRU.</p> <p>Исследование корректности систем защиты; методология обследования и проектирования систем защиты</p> <p>Концепция защищенного ядра; методы верификации; защищенные домены. Модель Белла-Лападулы.</p>

	<p>Ролевая политика безопасности. Модель политики контроля целостности; управление процессами функционирования систем защиты. Роль стандартов информационной безопасности. Стандарты по оценке защищенных систем. Европейские критерии безопасности информационных технологий.</p> <p>Федеральные критерии безопасности информационных технологий. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; примеры практической реализации; построение парольных систем. Единые критерии безопасности информационных технологий. Анализ стандартов информационной безопасности.</p>
<b>Форма промежуточной аттестации:</b>	Зачет

<b>Название:</b>		Б1.В.ОД.9. Социально-психологические проблемы управления персоналом
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ОК-1, ОПК-1, ПК-12
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основные направления и концепции научных исследований</li> <li>– методологию и методы проведения получения нового знания</li> <li>– выбор методов и средств, разработка инструментария эмпирического исследования, сбор, обработка, анализ, оценка и интерпретация полученных результатов исследования</li> <li>– инструментальные возможности современных прикладных программных продуктов, модели нарушителя и лояльного сотрудника в сфере ИБ.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– обобщать, интерпретировать и критически оценивать результаты, полученные отечественными и зарубежными исследователями</li> <li>– применять методы поиска, обработки научно-аналитической информации и системный подход к написанию исследовательских работ по финансовой и экономической тематикам;</li> <li>– обобщать и проводить критический анализ результатов, полученных отечественными и зарубежными учеными в определенной области научного знания, выявлять и формулировать актуальные научные проблемы</li> <li>– обосновывать актуальность, теоретическую и практическую значимость темы научного исследования, разрабатывать планы и программы проведения научного исследования;</li> <li>– применять возможности современных информационных технологий в различных областях человеческой деятельности.</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– самостоятельной работы, самоорганизации и организации выполнения поручений;</li> <li>– владения культурой критического мышления, навыками к обобщению, анализу, восприятию научно-аналитической информации, постановке цели и выбору путей её достижения.</li> <li>– владеть техникой самостоятельного управления несложными проектами, командной работы в проектах;</li> <li>– пользования организационным инструментарием управления проектами;</li> <li>– применения на практике методов противодействия рискам</li> <li>– работы с нормативной документацией по обеспечению информационной безопасности;</li> <li>– методами проектного анализа и математическим аппаратом оценки эффективности и рисков проекта;</li> </ul>
<b>Содержание:</b>		Понятие о лояльном сотруднике и нарушителе в информационной сфере. Построение психологического

	<p>портрета. Возможные способы построения.          Представления о чертах характера возможного нарушителя и лояльного сотрудника. Верные и неверные представления.          Модели возможного нарушителя и лояльного сотрудника.          Характерологические черты лояльного сотрудника в ИБ.          Психологический портрет лояльного сотрудника. Социально-психологические миры.          Стереотипы мышления и поведения. Личность и ложная личность.</p>
<p><b>Форма промежуточной аттестации:</b></p>	<p>Зачет</p>

<b>Название:</b>		Б1.В.ДВ.1.1. Противодействие техническим разведкам
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-7, ПК-14, ПК-15
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>▪ основные методы разработки алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов;</li> <li>▪ основные задачи анализа алгоритмов;</li> <li>▪ технические каналы утечки информации;</li> <li>▪ возможности технических средств перехвата информации;</li> <li>▪ способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;</li> <li>▪ организацию защиты информации от утечки по техническим каналам на объектах информатизации.</li> </ul>
	<b>уметь:</b>	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
	<b>владеть навыками /иметь опыт:</b>	безопасного использования технических средств в профессиональной деятельности.
<b>Содержание:</b>		Механизмы и технологии технической разведки. Системный подход к формированию общих принципов и основных способов противодействия техническим разведкам. Скрытие демаскирующих признаков. Противодействие радио и радиотехнической разведке. Физические и технические основы противодействия видовой разведке. Технический контроль защиты объектов от утечки информации за счет побочных электромагнитных излучений. Организация службы безопасности; функции, задачи и направления деятельности.
<b>Форма промежуточной аттестации:</b>		Зачет

<b>Название:</b>		Б1.В.ДВ.1.2. Компьютерные схмотехнологии
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-7, ПК-14, ПК-15
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>▪ важнейшие этапы и тенденции в развитии элементной базы ЭВМ;</li> <li>▪ основные дискретные элементы вычислительных систем; интегральные элементы и основные функциональные узлы ЭВМ;</li> <li>▪ принципы функционирования и взаимодействия основных узлов ЭВМ;</li> <li>▪ принципы построения и особенности функционирования источников питания ЭВМ;</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>▪ изложить основные принципы организации БИС/СБИС программируемой структуры, микропроцессорных комплектов и памяти</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>▪ методами оценки параметров функционирования элементов, узлов ЭВМ и отдельных устройств.</li> <li>▪ работы с различными средствами вычислительной техники</li> </ul>
<b>Содержание:</b>		<p>Совместная работа цифровых элементов в составе узлов и устройств: типы выходных каскадов, цепи питания, согласование связей, элементы задержки, формирователи импульсов, элементы индикации, оптоэлектронные развязки; триггеры; Синхронизация в цифровых устройствах; риски сбоя в комбинационных и последовательных схемах; функциональные узлы комбинационного типа; функциональные узлы последовательностного типа: регистры, счетчики, распределители;</p> <p>Матричные умножители; БИС/СБИС с программируемой структурой: программируемые логические матрицы, программируемая матричная логика, базовые матричные кристаллы, оперативно перестраиваемые FPGA; Схмотехника запоминающих устройств: статические, динамические, масочные, прожигаемые; запоминающие устройства на основе БИС/СБИС;</p> <p>Микропроцессорные комплекты БИС/СБИС; автоматизация функционально-логического этапа проектирования цифровых узлов и устройств.</p>
<b>Форма промежуточной аттестации:</b>		зачет

<b>Название:</b>		Б1.В.ДВ.2.1. Организационно-правовые механизмы обеспечения информационной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):</b>		ПК-3, ПК-14, ПК-16
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– об информационном праве как основе информационного общества, содержание основных понятий по правовому обеспечению информационной безопасности;</li> <li>– правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;</li> <li>– понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;</li> <li>– основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; правила лицензирования и сертификации в области защиты информации.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;</li> <li>– применять действующую законодательную базу в области информационной безопасности;</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	– разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов, иметь навыки работы с нормативно-правовыми актами.
<b>Содержание:</b>		Информация как объект правового регулирования Законодательство РФ в области информационной безопасности Информационная безопасность личности. Информационная безопасность общества. Информационная безопасность государства Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Компьютерные правонарушения. Обеспечение безопасности в глобальном информационном пространстве. Международное законодательство в области защиты информации. Ответственность в информационной сфере. Правовое регулирование проведения оперативно-розыскных мероприятий.
<b>Форма промежуточной аттестации:</b>		зачет

<b>Название:</b>		Б1.В.ДВ.2.2. Стандарты в сфере информационной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-3, ПК-14, ПК-16
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основные стандарты, регламентирующие управление ИБ;</li> <li>– принципы разработки процессов управления ИБ;</li> <li>– подходы к интеграции системы управления информационной безопасностью (СУИБ) в общую систему управления предприятием.</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ;</li> <li>– определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;</li> <li>– применять процессный подход к управлению ИБ в различных сферах деятельности;</li> <li>– используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;</li> <li>– практически решать задачи формализации разрабатываемых процессов управления ИБ;</li> <li>– разрабатывать и внедрять СУИБ и оценивать ее эффективность.</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– терминологией и процессным подходом построения систем управления ИБ;</li> <li>– навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;</li> <li>– навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.</li> </ul>
<b>Содержание:</b>		Введение. Базовые вопросы управления Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ ИБ. Процессный подход Основные процессы СУИБ. Обязательная документация СУИБ Эксплуатация и независимый аудит СУИБ. Внедрение разработанных процессов. Документ «Положение о применимости» Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса» Обеспечение соответствия требованиям законодательства РФ
<b>Форма промежуточной аттестации:</b>		Зачет



<b>Название:</b>		Б1.В.ДВ.3.1. Теория систем и системный анализ
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):</b>		ПК-3, ПК-6
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>▪ Методы и способы поиска требуемой информации, в том числе в глобальных сетях;</li> <li>▪ сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>▪ Критически анализировать имеющуюся информацию, в том числе методы системного анализа;</li> <li>▪ проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>▪ Поиска нужной информации и проведения сравнительного анализа полученных данных;</li> <li>▪ проектирования сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты</li> </ul>
<b>Содержание:</b>		<p>Определение системы. Виды и формы представления структур. Параметры характеризующие систему. Методы и модели теории систем. Понятие цели и закономерности целеобразования. Закономерности теории систем. Классификация систем. Понятие системного анализа. Экспертные оценки. Методики представления систем.</p>
<b>Форма промежуточной аттестации:</b>		Зачет

<b>Название:</b>		Б1.В.ДВ.3.2. Общая теория систем
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-3, ПК-6
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>▪ методы и модели теории систем и системного анализа, закономерности построения, функционирования и развития систем целеобразования;</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>▪ выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>▪ выбора способов и процедур использования различных математических и алгоритмических методов в процессе анализа систем;</li> <li>▪ навыками работы с инструментами системного анализа</li> </ul>
<b>Содержание:</b>		Понятие системы. Параметры, характеризующие систему. Закономерности теории систем. Классификация систем. Понятие системного анализа. Методики представления систем. Экспертные оценки. Методы сложных экспертиз.
<b>Форма промежуточной аттестации:</b>		Зачет

<b>Название:</b>		Б1.В.ДВ.4.1. Проектирование защищенных баз данных
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-6, ПК-7, ПК-8
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	<ul style="list-style-type: none"> <li>– основы построения защищённых баз данных;</li> <li>– концепцию защиты информации в проектируемых базах данных;</li> <li>– основные принципы и методы защиты информации в процессе проектирования баз данных;</li> <li>– основные руководящие и нормативные документы по защите информации в проектируемых базах данных;</li> <li>– порядок организации защиты информации в процессе проектируемых баз данных</li> </ul>
	<b>уметь:</b>	<ul style="list-style-type: none"> <li>– выявлять угрозы каналы утечки информации в процессе проектирования баз данных;</li> <li>– описывать (моделировать) объекты защиты и угрозы безопасности информации в проектировании баз данных;</li> <li>– применять наиболее эффективные методы и средства защиты информации в процессе проектирование баз данных;</li> <li>– контролировать эффективность мер защиты</li> </ul>
	<b>владеть навыками /иметь опыт:</b>	<ul style="list-style-type: none"> <li>– Выявления угроз безопасности информации в базах данных;</li> <li>– Обеспечения оптимального уровня защиты информации в проектируемых базах данных</li> </ul>
<b>Содержание:</b>		<p>Этапы развития информационных систем. Основные понятия баз данных. Особенности современных АС и требования законодательства по защите данных при автоматизированной обработке. Архитектура многопользовательских систем. Риски информационной безопасности.</p> <p>Моделирование предметной области. OLTP и OLAP-системы. Проектирование защищенной БД: основные этапы. Особенности даталогических моделей. Составление технического задания для проектирования базы данных. Основные виды графических нотаций. Создание баз данных в СУБД Access, MS SQL, Oracle , ввод и редактирование данных. Типы данных в БД.</p> <p>Основы реляционной алгебры. Реляционные исчисления, построенные на доменах и кортежах.</p> <p>СУБД Access. Запросы. в СУБД Access и Oracle на основе языка QBEи SQL</p> <p>Организация поиска, фильтрации, сортировки средствами СУБД Access.</p> <p>Этапы и принципы проектирования баз данных. Формирование требований пользователей информационной системы во время проектирования.</p> <p>Повышение производительности запросов в БД. Планы выполнения запросов. Многопользовательский доступ. Транзакция. Управление транзакциями в СУБД Oracle, MS SQL.</p>

	<p>Механизмы блокировки. Индексы. Администраторы базы данных и их функции. Разграничение обязанностей. Правило второй руки. Средства защиты данных от привилегированных пользователей Разработка нормативно- распорядительной документации для управления доступом к данным в БД. Резервное копирование, аудит. Методы шифрования БД.</p>
<b>Форма промежуточной аттестации:</b>	зачет

<b>Название:</b>		Б1.В.ДВ.4.1. Системы искусственного интеллекта
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-6, ПК-7, ПК-8
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	модели представления и методы обработки знаний, системы принятия решений; Методы направленного перебора и выбора альтернативных вариантов
	<b>уметь:</b>	разрабатывать математические модели процессов и объектов, методы их исследования, выполнять их сравнительный анализ; сочетать методы искусственного интеллекта с обычными методами анализа предметной области с учетом своих личных качеств применять методы направленного перебора и выбора альтернативных вариантов использовать методы искусственного интеллекта для построения модели угроз и рисков использовать методы искусственного интеллекта для анализа систем
	<b>владеть навыками /иметь опыт:</b>	способами формализации
<b>Содержание:</b>		Основные понятия искусственного интеллекта. Базы данных и знаний. Основные области применения и задачи интеллектуальных систем. Классификация интеллектуальных систем Проблема представления знаний. Методы представления знаний. Продукционные системы. Фреймы. Исчисление предикатов. Нейронные сети. Генетические алгоритмы Языки искусственного интеллекта. Обзор языков представления знаний. Понятие о функциональном программировании. Язык ЛИСП. Понятие о логическом программировании. Язык Пролог. Экспертные системы (ЭС). Искусственный интеллект и естественный язык. Понимание выражений естественного языка. Представление лингвистических знаний. Методы анализа и синтеза текста. ИИ и прикладная лингвистика.
<b>Форма промежуточной аттестации:</b>		зачет

<b>Название:</b>		ФТД.1 Методы математического планирования эксперимента в системах информационной безопасности
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-7
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	модели представления и методы обработки знаний, системы принятия решений; Методы направленного перебора и выбора альтернативных вариантов
	<b>уметь:</b>	разрабатывать математические модели процессов и объектов, методы их исследования, выполнять их сравнительный анализ; сочетать методы искусственного интеллекта с обычными методами анализа предметной области с учетом своих личных качеств применять методы направленного перебора и выбора альтернативных вариантов использовать методы искусственного интеллекта для построения модели угроз и рисков использовать методы искусственного интеллекта для анализа систем
	<b>владеть навыками /иметь опыт:</b>	способами формализации
<b>Содержание:</b>		Основные понятия искусственного интеллекта. Базы данных и знаний. Основные области применения и задачи интеллектуальных систем. Классификация интеллектуальных систем Проблема представления знаний. Методы представления знаний. Продукционные системы. Фреймы. Исчисление предикатов. Нейронные сети. Генетические алгоритмы Языки искусственного интеллекта. Обзор языков представления знаний. Понятие о функциональном программировании. Язык ЛИСП. Понятие о логическом программировании. Язык Пролог. Экспертные системы (ЭС). Искусственный интеллект и естественный язык. Понимание выражений естественного языка. Представление лингвистических знаний. Методы анализа и синтеза текста. ИИ и прикладная лингвистика.
<b>Форма промежуточной аттестации:</b>		зачет

<b>Название:</b>		Б1.В.ДВ.4.1. Безопасность информационного и программного обеспечения автоматизированных систем
<b>Название и номер направления и/или специальности:</b>		10.04.01 Информационная безопасность
<b>Компетенции обучающегося, формируемые в результате освоения дисциплины :</b>		ПК-2
<b>Результаты освоения дисциплины</b>	<b>знать:</b>	- методы и средства анализа информационного и программного обеспечения; - основы построения защищенных информационного и программного обеспечения.
	<b>уметь:</b>	- пользоваться средствами анализа безопасности информационного и программного обеспечения; - анализировать и оценивать угрозы информационной безопасности информационного и программного обеспечения.
	<b>владеть навыками /иметь опыт:</b>	- методами и средствами анализа безопасности информационного и программного обеспечения; - разработка безопасного информационного и программного обеспечения.
<b>Содержание:</b>		<p>Основные понятия искусственного интеллекта. Базы данных и знаний. Основные области применения и задачи интеллектуальных систем. Классификация интеллектуальных систем</p> <p>Проблема представления знаний. Методы представления знаний.</p> <p>Продукционные системы. Фреймы. Исчисление предикатов. Нейронные сети. Генетические алгоритмы</p> <p>Языки искусственного интеллекта. Обзор языков представления знаний. Понятие о функциональном программировании. Язык ЛИСП. Понятие о логическом программировании. Язык Пролог.</p> <p>Экспертные системы (ЭС).</p> <p>Искусственный интеллект и естественный язык. Понимание выражений естественного языка. Представление лингвистических знаний. Методы анализа и синтеза текста. ИИ и прикладная лингвистика.</p>
<b>Форма промежуточной аттестации:</b>		зачет