Аннотации рабочих программ дисциплин
по направлению подготовки
10.04.01 «Информационная безопасность»

	Название:	Б1.Б.1. Защищенные информационные системы
	Название и номер направления и/или специальности:	10.04.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины :	ОК-2; ПК-4; ПК-7
Результаты освоения дисциплины	**знать:**	– основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; – основные методы и средства обеспечения безопасности операционных систем; – основные методы и средства обеспечения сетевой безопасности; – основные методы и средства обеспечения безопасности в системах управления базами данных;
	уметь:	осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;
	владеть навыками /иметь опыт:	настройки подсистем защиты основных операционных систем.
	Содержание:	Защита в операционных системах. Механизмы защиты операционной системы Интеграция защищенных операционных систем. Типовые угрозы сетевой безопасности. Методы и средства обеспечения информационной безопасности в вычислительных сетях. Защита в системах управления базами данных. Теоретические основы безопасности в СУБД
	Форма промежуточной аттестации:	Экзамен Курсовой проект

	Название:	Б1.Б.2. Технология обеспечения информационной безопасности
	Название и номер направления и/или специальности:	10.04.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-2; ПК-2, ПК-14
Результаты освоения дисциплины	**знать:**	– место и роль информационной безопасности в системе национальной безопасности Российской Федерации; – методы концептуального проектирования технологий обеспечения информационной безопасности; – принципы построения информационных систем; – принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; – принципы организации информационных систем в соответствии с требованиями по защите информации.
	уметь:	– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – осуществлять меры противодействия нарушениям сетевой

		безопасности с использованием различных программных и аппаратных средств защиты. – анализировать и оценивать угрозы информационной безопасности объекта; – осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; – обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; – организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;
	владеть навыками /иметь опыт:	– навыками выявления и уничтожения компьютерных вирусов; – методами и средствами выявления угроз безопасности автоматизированным системам; – методами анализа и формализации информационных процессов объекта и связей между ними; – пользования профессиональной терминологией.
Содержание:		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 безопасности.
Форма промежуточной аттестации:		Зачет

Название:		Б1.Б.3. Управление информационной безопасностью
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ОК-1; ОПК-2; ПК-13; ПК-15
Результаты освоения дисциплины	**знать:**	методы и средства управления информационной безопасностью;
	уметь:	– проводить общую самооценку соответствия организации требованиям нормативных документов и Стандартам по информационной безопасности; – выявлять и анализировать характеристики возможных угроз и каналов утечки информации;
	владеть навыками /иметь опыт:	– навыками управления информационной безопасностью простых объектов – работы с нормативной документацией по обеспечению информационной безопасности; – работы с программно-аппаратными средствами обеспечения информационной безопасности
Содержание:		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. 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. 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. Слежение за доступом к системам и их использованием Разработка и сопровождение информационных систем. Требования к 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.
Форма промежуточной аттестации:	Экзамен Курсовая работа

Название:		Б1.Б.4. Информационные технологии в науке и производстве
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ОК-2; ОПК-1; ПК-1
Результаты освоения дисциплины	**знать:**	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
	уметь:	строить математическую модель задачи, подбирать метод ее решения, находить оптимальное решение и делать содержательную интерпретацию.
	владеть навыками /иметь опыт:	пользования терминологией исследования операций и соответствующим математическим аппаратом.
Содержание:		Общие вопросы ИО. Календарное планирование программ сетевыми методами. Теория игр. Теория массового обслуживания. Имитационное моделирование
Форма промежуточной аттестации:		Зачет

Название:		Б1.Б.5. Экономика и управление
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ОК-2, ПК-1, ПК-16
Результаты освоения дисциплины	**знать:**	– основные теории и методы макро- и микроэкономики – экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности); – современные формы и методы хозяйствования, нормативные правовые акты, регламентирующие деятельность предприятия; – социально-экономический и административно-хозяйственный механизм производственного процесса и понимать сущность деятельности предприятия; – основные экономические показатели деятельности предприятий и показатели оценки; – эффективности использования ресурсов предприятия.
	уметь:	– анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности; – рассчитывать показатели эффективности использования производственных ресурсов предприятия; – анализировать и оценивать экономические показатели деятельности предприятия и влияние на них принимаемых менеджерами решений.
	Владеть навыками /иметь опыт:	– приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям; – практическими навыками решения конкретных технико-экономических и управленческих вопросов в области автоматизации технологических процессов и производств; – находить организационно - управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность
Содержание:		1. Предприятие как субъект и объект предпринимательской деятельности. 2. Прибыль предприятия. 3. Налогообложение предприятий 4. Производственные ресурсы предприятия. Основной капитал 5. Производственные ресурсы предприятия. Оборотный капитал 6. Производственные ресурсы предприятия. Трудовые ресурсы 7. Издержки производства и себестоимость продукции предприятия. 8. Эффективность хозяйственной деятельности. 9. Функции и методы управления производством 10. Процесс принятия управленческих решений и ответственность менеджеров всех уровней
Форма промежуточной аттестации:		Экзамен

Название:		Б1.В.ОД.1. Философия и методология научного исследования
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-5, ПК-6, ПК-8
Результаты освоения дисциплины	**знать:**	- основные методологические принципы научного исследования; - методы научного исследования; - структуру и содержание этапов исследовательского процесса; - методические требования к структуре и содержанию научного исследования; - правила и требования к оформлению диссертации.
	уметь:	- квалифицированно ориентироваться в методологическом обеспечении исследования на философском, общенаучном, частно-научном и методическом уровнях познания; - формулировать решаемую проблему, определять объект и предмет исследования, ставить исследовательские задачи и разрабатывать план их решения; - разрабатывать программу исследования; - формулировать структуру и содержание этапов исследовательского процесса; - выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования. - формулировать и решать задачи, возникающие в ходе научно-исследовательской деятельности; - осуществлять поиск информации, необходимой для написания научной работы; - оформлять и представлять результаты проведённой исследовательской работы.
	владеть навыками /иметь опыт:	- использования достижений и основных понятий теории методологии науки для проведения самостоятельных научных исследований; - владеть приёмами постановки целей и задач научных и проектных исследований; - самостоятельной работы с литературой для поиска информации; - оформления и представления результатов проведённой исследовательской работы.
Содержание:		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. Сбор научной информации. Основные источники информации. Оформление научных исследований. Методология диссертационного исследования
Форма промежуточной аттестации:		Экзамен

	Название:	Б1.В.ОД.2. Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности
	Название и номер направления и/или специальности:	10.04.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины :	ПК-3, ПК-14, ПК-16
Результаты освоения дисциплины	**знать:**	– законодательства об обеспечении безопасности государства, содержание основных понятий по правовому обеспечению безопасности государства; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений государства и граждан в области обеспечения безопасности государства.
	уметь:	– отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
	владеть навыками /иметь опыт:	– применять действующую законодательную базу в области информационной безопасности; – 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.
	Содержание:	Правовой аспект проблемы общей теории безопасности РФ. Информационное противоборство как новый вид межгосударственной борьбы. Общий состав мер по обеспечению безопасности государства. Ограничение прав и свобод человека при обеспечении безопасности государства. Методологические основы и понятийный аппарат общей теории безопасности государства. Место общей теории безопасности государства в системе научных знаний. Основные понятия общей теории безопасности государства Система правового обеспечения общей теории безопасности РФ. Основные источники угроз национальной безопасности РФ. Международно-правовые основы деятельности государств по обеспечению безопасности. Ответственность за нарушение законодательства в сфере обеспечения безопасности государства. Государственная тайна и ее правовой статус.
	Форма промежуточной аттестации:	Экзамен Курсовой проект

	Название:	Б1.В.ОД.3. Методы и средства защиты информации в системах электронного документооборота
	Название и номер направления и/или специальности:	10.04.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины :	ПК-8, ПК-16
Результаты освоения дисциплины	**знать:**	– основные понятия и принципы делопроизводства и электронного документооборота; – принципы функционирования автоматизированных систем поддержки документооборота и обеспечения их безопасности; – особенности сертификации и аттестации систем электронного документооборота по требованиям безопасности;
	уметь:	– классифицировать и оценивать угрозы информационной безопасности для систем электронного документооборота; – разрабатывать модели угроз и модели нарушителя безопасности систем электронного документооборота;
	владеть навыками /иметь опыт:	– анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в системах электронного документооборота; – пользования методами и средствами выявления угроз безопасности системам электронного документооборота.
	Содержание:	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.
	Форма промежуточной аттестации:	Экзамен

	Название:	Б1.В.ОД.4. Проектирование технических средств и систем в защищенном исполнении
	Название и номер направления и/или специальности:	10.04.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ПК-2, ПК-3, ПК-7
Результаты освоения дисциплины	**знать:**	- основные понятия, используемые при обеспечении информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении; - взаимосвязь обеспечения информационной безопасности с технологиями проектирования и создания (модернизации) объектов информатизации; - средства видов обеспечений компьютерной системы, подлежащие разработке при проектировании, создании (модернизации) компьютерной системы; - основные мероприятия по организации разработке средств видов обеспечения компьютерной системы, отвечающих требованиям информационной безопасности; - общие требования к технологической безопасности средств

		программного и информационного обеспечений компьютерных систем; - структуру и содержание программы обеспечения информационной безопасности проектирования, создания (модернизации) компьютерных систем в составе объектов информатизации; - требования к разработке средств основных видов обеспечения компьютерной системы в защищенном исполнении; - требования по обеспечению информационной безопасности стенда для разработки средств программного и информационного обеспечения; - требования информационной безопасности к документации на объекты информатизации на базе компьютерных систем; - структуру, цели создания, назначение и основные функции системы обеспечения информационной безопасности проектирования, создания (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении;
	уметь:	- определять основные мероприятия по организации разработки средств видов обеспечения компьютерной системы; - разработать требования к технологической безопасности средств программного и информационного обеспечения; - разрабатывать структуру и отдельные разделы программы обеспечения информационной безопасности проектирования, создания (модернизации) компьютерной системы в защищенном исполнении в составе объекта информатизации; - разрабатывать документы, регламентирующие обеспечение информационной безопасности разработки объектов информатизации на базе компьютерных систем в защищенном исполнении;
	владеть навыками /иметь опыт:	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;
Содержание:		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.
Форма промежуточной аттестации:		Экзамен

Название:		Б1.В.ОД.5. Теоретические основы управления
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-2, ПК-12, ПК-13
Результаты освоения дисциплины	**знать:**	методы анализа, синтеза, способы математического моделирования и основные подходы к организации современных систем управления; особенности цифровых систем управления.
	уметь:	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.
	владеть навыками /иметь опыт:	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
Содержание:		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.
Форма промежуточной аттестации:		Зачет с оценкой

Название:		Б1.В.ОД.6. Информационно-аналитические системы безопасности
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-1, ПК-6, ПК-8
Результаты	**знать:**	характеристики современного информационного общества, проблем защиты информации и обеспечения информационной безопасности;
	уметь:	– 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;
	владеть навыками /иметь опыт:	– 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.
Содержание:		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.
Форма промежуточной аттестации:		Экзамен

Название:		Б1.В.ОД.7. Иностранный язык в профессиональной сфере
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ОПК-1, ПК-6
Результаты освоения дисциплины	**знать:**	– особенности иноязычного общения в типичных ситуациях, связанных с деловой поездкой за рубеж; – нормы невербального делового общения; – структуру фирмы/компании, названия должностей персонала; – структуру CV, резюме, договора.
	уметь:	– вести диалоги этикетного характера, используя вербальные и невербальные средства вежливого поведения на ИЯ; – использовать свой речевой аппарат общения коммуникативно приемлемо и правильно в ситуациях социально-культурного и делового общения при: – знакомстве, представлении, личной встрече или разговоре по телефону с партнером по бизнесу, представлении другого лица; – подготовке к служебной поездке за рубеж (заказ авиабилета, онирование номера в гостинице); – прибытии в страну делового партнера (таможенный контроль, у администратора в гостинице, ориентация по городу, заказ блюд в ресторане и т.п.); – представлении фирмы/продукции/услуг; – подписании договора о поставках, сотрудничестве; – ориентироваться в структуре делового письма и извлекать основную информацию из текста деловой корреспонденции; – написать CV, резюме, деловое письмо с соблюдением общепринятых норм.

	владеть навыками /иметь опыт:	– 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).
Содержание:		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.
Форма промежуточной аттестации:		Экзамен

Название:		Б1.В.ОД.8. Теоретические основы компьютерной безопасности
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-2, ПК-4, ПК-7
Результаты освоения дисциплины	**знать:**	– методологические и технологические основы комплексного обеспечения безопасности АС, – угрозы и методы нарушения безопасности АС, – формальные модели, лежащие в основе систем защиты АС, – стандарты по оценке защищенности АС и их теоретические основы, – методы и средства реализации защищенных АС, методы и средства верификации и анализа надежности защищенных АС;
	уметь:	– проводить анализ АС с точки зрения обеспечения компьютерной безопасности, – разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы, – применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС, – реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС;
	владеть навыками /иметь опыт:	– работы с АС распределенных вычислений и обработки информации; – работы с документацией АС, – использования критериев оценки защищенности АС, – построения формальных моделей систем защиты информации АС.
Содержание:		Основне понятия теории компьютерной информации. Архитектура электронных систем обработки данных. Модели безопасности. Анализ угроз информационной безопасности. Анализ причин нарушений безопасности. Изъяны защиты. Структура теории безопасности. Уровни защиты информации. 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. Особенности реализации систем с симметричными и несимметричными ключами. Цифровая подпись. Построение систем защиты от угрозы раскрытия параметров информационной системы. Методология построения защищенных систем. Политика безопасности. Методы построения защищенных автоматизированных систем. Формальные модели безопасности. Модель матрицы доступов HRU. Исследование корректности систем защиты; методология обследования и проектирования систем защиты Концепция защищенного ядра; методы верификации; защищенные домены. Модель Белла-Лападулы. 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. 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.
Форма промежуточной аттестации:	Зачет

Название:		Б1.В.ОД.9. Социально-психологические проблемы управления персоналом
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ОК-1, ОПК-1, ПК-12
Результаты освоения дисциплины	**знать:**	– основные направления и концепции научных исследований – методологию и методы проведения получения нового знания – выбор методов и средств, разработка инструментария эмпирического исследования, сбор, обработка, анализ, оценка и интерпретация полученных результатов исследования – инструментальные возможности современных прикладных программных продуктов, модели нарушителя и лояльного сотрудника в сфере ИБ.
	уметь:	– обобщать, интерпретировать и критически оценивать результаты, полученные отечественными и зарубежными исследователями – применять методы поиска, обработки научно-аналитической информации и системный подход к написанию исследовательских работ по финансовой и экономической тематикам; – обобщать и проводить критический анализ результатов, полученных отечественными и зарубежными учеными в

		определенной области научного знания, выявлять и формулировать актуальные научные проблемы – обосновывать актуальность, теоретическую и практическую значимость темы научного исследования, разрабатывать планы и программы проведения научного исследования; – применять возможности современных информационных технологий в различных областях человеческой деятельности.
	владеть навыками /иметь опыт:	– самостоятельной работы, самоорганизации и организации выполнения поручений; – владения культурой критического мышления, навыками к обобщению, анализу, восприятию научно-аналитической информации, постановке цели и выбору путей её достижения. – владеть техникой самостоятельного управления несложными проектами, командной работы в проектах; – пользования организационным инструментарием управления проектами; – применения на практике методов противодействия рискам – работы с нормативной документацией по обеспечению информационной безопасности; – методами проектного анализа и математическим аппаратом оценки эффективности и рисков проекта;
Содержание:		Понятие о лояльном сотруднике и нарушителе в информационной сфере. Построение психологического 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.
Форма промежуточной аттестации:		Зачет

Название:		Б1.В.ДВ.1.1. Противодействие техническим разведкам
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-7, ПК-14, ПК-15
Результаты освоения дисциплины	**знать:**	▪ основные методы разработки алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; ▪ основные задачи анализа алгоритмов; ▪ технические каналы утечки информации; ▪ возможности технических средств перехвата информации; ▪ способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; ▪ организацию защиты информации от утечки по техническим каналам на объектах информатизации.
	уметь:	проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе

		автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
	владеть навыками /иметь опыт:	безопасного использования технических средств в профессиональной деятельности.
Содержание:		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.
Форма промежуточной аттестации:		Зачет

Название:		Б1.В.ДВ.1.2. Компьютерные схемотехнологии
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-7, ПК-14, ПК-15
Результаты освоения дисциплины	**знать:**	▪ важнейшие этапы и тенденции в развитии элементной базы ЭВМ; ▪ основные дискретные элементы вычислительных систем; интегральные элементы и основные функциональные узлы ЭВМ; ▪ принципы функционирования и взаимодействия основных узлов ЭВМ; ▪ принципы построения и особенности функционирования источников питания ЭВМ;
	уметь:	▪ изложить основные принципы организации БИС/СБИС программируемой структуры, микропроцессорных комплектов и памяти
	владеть навыками /иметь опыт:	▪ методами оценки параметров функционирования элементов, узлов ЭВМ и отдельных устройств. ▪ работы с различными средствами вычислительной техники
Содержание:		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; Матричные умно жители; БИС/СБИС с программируемой структурой: программируемые логические матрицы, программируемая матричная логика, базовые матричные кристаллы, оперативно перестраиваемые FPGA; Схемотехника запоминающих устройств: статические, динамические, масочные, прожигаемые; запоминающие устройства на основе БИС/СБИС; Микропроцессорные комплекты БИС/СБИС; автоматизация функционально-логического этапа проектирования цифровых узлов и устройств.
Форма промежуточной аттестации:		зачет

Название:		Б1.В.ДВ.2.1. Организационно-правовые механизмы обеспечения информационной безопасности
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-3, ПК-14, ПК-16
Результаты освоения дисциплины	**знать:**	– об информационном праве как основе информационного общества, содержание основных понятий по правовому обеспечению информационной безопасности; – правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; – понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; – основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; правила лицензирования и сертификации в области защиты информации.
	уметь:	– отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; – применять действующую законодательную базу в области информационной безопасности;
	владеть навыками /иметь опыт:	– 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.
Содержание:		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.
Форма промежуточной аттестации:		зачет

Название:		Б1.В.ДВ.2.2. Стандарты в сфере информационной безопасности
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-3, ПК-14, ПК-16
Результаты освоения дисциплины	**знать:**	– основные стандарты, регламентирующие управление ИБ; – принципы разработки процессов управления ИБ; – подходы к интеграции системы управления информационной безопасностью (СУИБ) в общую систему управления предприятием.
	уметь:	– анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; – определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; – применять процессный подход к управлению ИБ в различных сферах деятельности; – используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; – практически решать задачи формализации разрабатываемых процессов управления ИБ; – разрабатывать и внедрять СУИБ и оценивать ее эффективность.
	владеть навыками /иметь опыт:	– терминологией и процессным подходом построения систем управления ИБ; – навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; – навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
Содержание:		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
Форма промежуточной аттестации:		Зачет

Название:		Б1.В.ДВ.3.1. Теория систем и системный анализ
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-3, ПК-6
Результаты освоения дисциплины	**знать:**	▪ Методы и способы поиска требуемой информации, в том числе в глобальных сетях; ▪ сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты
	уметь:	▪ Критически анализировать имеющуюся информацию, в том числе методы системного анализа; ▪ проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты
	владеть навыками /иметь опыт:	▪ Поиска нужной информации и проведения сравнительного анализа полученных данных; ▪ проектирования сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты
Содержание:		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.
Форма промежуточной аттестации:		Зачет

Название:		Б1.В.ДВ.3.2. Общая теория систем
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-3, ПК-6
Результаты освоения дисциплины	**знать:**	▪ методы и модели теории систем и системного анализа, закономерности построения, функционирования и развития систем целеобразования;
	уметь:	▪ выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления
	владеть навыками /иметь опыт:	▪ выбора способов и процедур использования различных математических и алгоритмических методов в процессе анализа систем; ▪ навыками работы с инструментами системного анализа
Содержание:		Понятие системы. Параметры, характеризующие систему. Закономерности теории систем. Классификация систем. Понятие системного анализа. Методики представления систем. Экспертные оценки. Методы сложных экспертиз.
Форма промежуточной аттестации:		Зачет

Название:		Б1.В.ДВ.4.1 Планирование эксперимента и обработка данных
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-6, ПК-7, ПК-8
Результаты освоения дисциплины	**знать:**	– о существующих программных продуктах, позволяющих производить обработку данных; – о видах экспериментов и методах обработки данных; – понятие математических и статистических методов, об элементах теории вероятностей
	уметь:	– применять программные продукты статистической обработки данных; – применять на практике различные виды обработки данных; – существлять сбор, обработку, анализ и систематизацию научно-технической информации по планированию экспериментов и обработке данных
	владеть навыками /иметь опыт:	– использования инструментов статистического анализа и обработки данных; – рименения программных средств обработки данных; – азработки плана проведения научных экспериментов
Содержание:		Понятие математических и статистических методов. Элементы теории вероятностей. Статистическая вероятность. Основные понятия теории обработки статистической информации. Статистические распределения и их графические изображения. Общая схема статистического исследования. Генеральная, выборочная и статистическая совокупность. Понятие о законах распределения. Качественные и количественные показатели. Проблемы и перспективы использования математических и статистических методов в науке и образовании.Статистический анализ информации. Статистическая оценка параметров распределения. Проверка статистических гипотез. Доверительные границы. Показатель точности опытов. Проверка статистической гипотезы о законе распределения. Проверка согласия эмпирического распределения с нормальным законом. Этапы анализа данных. Проверка статистических гипотез. Шкалирование. Преобразование данных. Табличное и графическое представление данных.Планирование и реализация научного эксперимента. Корректность математической обработки результатов эксперимента. Планирование экспериментов. Этапы планирования экспериментов. Статистическое планирование экспериментов. Некоторые методы планирования экспериментов. Пассивный эксперимент. Активный эксперимент. Задача активного планирования экспериментов. Постановка полного факторного эксперимента.Основные математические методы и статистические критерии для обработки результатов научного эксперимента. Описательная статистика. Критерии парных различий. Непараметрические, параметрические критерии. Корреляционный

	анализ. Факторный анализ. Прогнозирование. Регрессионный анализ. Методы контроля качества. Многомерные методы.Математическое моделирование. Роль интегрированных систем обработки данных в учебном процессе, научной и исследовательской деятельности. Средства моделирования и анализа данных на компьютере. Методы визуализации данных. Современное программное обеспечение для математической и статистической обработки. Обзор пакетов по статистическому анализу данных. Принципы работы в статистических пакетах. Статистические программы общего назначения. Описательная статистика и математические методы в электронных таблицах.
Форма промежуточной аттестации:	зачет

Название:		Б1.В.ДВ.4.1. Системы искусственного интеллекта
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-6, ПК-7, ПК-8
Результаты освоения дисциплины	**знать:**	модели представления и методы обработки знаний, системы принятия решений; Методы направленного перебора и выбора альтернативных вариантов
	уметь:	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
	владеть навыками /иметь опыт:	способами формализации
Содержание:		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.
Форма промежуточной аттестации:		зачет

Название:	ФТД.1 Методы математического планирования эксперимента в системах информационной безопасности

Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-7
Результаты освоения дисциплины	**знать:**	модели представления и методы обработки знаний, системы принятия решений; Методы направленного перебора и выбора альтернативных вариантов
	уметь:	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
	владеть навыками /иметь опыт:	способами формализации
Содержание:		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.
Форма промежуточной аттестации:		зачет

Название:		Б1.В.ДВ.4.1. Безопасность информационного и программного обеспечения автоматизированных систем
Название и номер направления и/или специальности:		10.04.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины :		ПК-2
Результаты освоения дисциплины	**знать:**	- методы и средства анализа информационного и программного обеспечения; - основы построения защищенных информационного и программного обеспечения.
	уметь:	- пользоваться средствами анализа безопасности информационного и программного обеспечения; - анализировать и оценивать угрозы информационной безопасности информационного и программного обеспечения.
	владеть навыками /иметь опыт:	- методами и средствами анализа безопасности информационного и программного обеспечения;

		- разработка безопасного информационного и программного обеспечения.
Содержание:		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.
Форма промежуточной аттестации:		зачет