Аннотации рабочих программ дисциплин (модулей) образовательной программы по направлению подготовки 10.03.01 «Информационная безопасность», профиль подготовки №1 «Безопасность компьютерных систем»

	Название:	Философия
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОК-1
Результаты освоения дисциплины	**знать:**	основные разделы и направления философии, методы и приемы философского анализа проблем; специфику философии как способа познания и духовного освоения мира, основные разделы современного философского знания и исторические типы философии, философские проблемы и методы исследования, связь философии с другими научными дисциплинами;
	уметь:	анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию; планировать и осуществлять свою деятельность с учетом результатов этого анализа; логично формулировать, излагать и аргументировано отстаивать собственное видение проблем и способов их разрешения; использовать положения и категории философии для оценивания и анализа различных социальных тенденций, фактов и явлений; использовать в практической жизни философские и общенаучные методы мышления и исследования; демонстрировать способность и готовность к диалогу по проблемам общественного и мировоззренческого характера, способность к рефлексии;
	владеть навыками /иметь опыт:	навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений; навыками анализа и интерпретации текстов, имеющих философское содержание; навыками поиска, критического восприятия, анализа и оценки источников информации; приемами ведения дискуссии, полемики, диалога, устной и письменной аргументации, публичной речи; базовыми принципами и приемами философского познания.
	Содержание:	Философия, ее предмет и место в культуре человечества; философия Древнего мира; античная философия; средневековая философия; философия эпохи Возрождения; философия нового времени (XVII – XVIII вв); классический этап философии Нового времени; современная западная философия; русская философия; учение о бытии (онтология); учение о развитии; природа человека и смысл его существования; учение об обществе (социальная философия); ценность как способ освоения мира человеком (аксиология); проблема сознания; познание (гносеология); научное познание; философские проблемы науки и техники; будущее человечества (философский аспект).
	Форма промежуточной аттестации:	Экзамен

Название:	История
Название и номер	10.03.01 Информационная безопасность

направления и/или специальности:		
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-3
Результаты освоения дисциплины	**знать:**	– основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; – основные направления, проблемы, теории и методы истории; – движущие силы и закономерности исторического процесса; – место человека в историческом процессе, политической организации общества; – различные подходы к оценке и периодизации всемирной и отечественной истории; – основные этапы и ключевые события истории России и мира с древности до наших дней; – выдающихся деятелей отечественной и всеобщей истории; – важнейшие достижения культуры и системы ценностей, сформировавшиеся в ходе исторического развития.
	уметь:	– логически мыслить, вести научные дискуссии; работать с разноплановыми источниками; – осуществлять эффективный поиск информации и критики источников; – получать, обрабатывать и сохранять источники информации; – преобразовывать информацию в знание, осмысливать процессы, события и явления в России и мировом сообществе в их динамике и взаимосвязи, руководствуясь принципами научной объективности и историзма; – формировать и аргументировано отстаивать собственную позицию по различным проблемам истории; – соотносить общие исторические процессы и отдельные факты; – выявлять существенные черты исторических процессов, явлений и событий; – извлекать уроки из исторических событий и на их основе принимать осознанные решения; применять терминологию исторической науки в профессиональной деятельности. –
	владеть навыками /иметь опыт:	– навыками критического восприятия информации; – представлениями о событиях российской и всемирной истории, основанными на принципе историзма; – навыками анализа исторических источников; – приемами ведения дискуссии и полемики.
Содержание:		Русь в древности и в эпоху европейского средневековья (IX-XVII вв.). Российская империя и мир в XVIII - начале XX вв.: попытки модернизации и промышленный переворот. Россия и мир в XX - XXI веках.
Форма промежуточной аттестации:		зачет

Название:	Иностранный язык
Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОК-7, ОК-8, ОПК-4

Результаты освоения дисциплины	**знать:**	лексический минимум в объеме 4000 учебных лексических единиц общего и терминологического характера (для иностранного языка); значение новых лексических единиц, связанных с тематикой данного этапа обучения и соответствующими ситуациями общения, в том числе оценочной лексики, реплик-клише речевого этикета, отражающих особенности культуры стран изучаемого языка; этапы процесса развития вычислительных систем и информационных технологий; значение изученных грамматических явлений (видовременные, неличные и неопределённо-личные формы глагола, формы условного наклонения, косвенная речь (косвенные вопросы), согласование времён и др.); особенности разговорного, литературного, профессионально-делового и публицистического стилей; страноведческую информацию из аутентичных источников. Сведения о стране/ странах изучаемого языка, их науке и культуре, исторических и современных реалиях, общественных деятелях, месте в мировом сообществе и мировой культуре.
	уметь:	использовать знания иностранного языка в профессиональной деятельности и межличностном общении; читать и переводить тексты общей, общетехнической, профессиональной направленности; *в диалогической речи:* участвовать в разговоре, беседе в ситуациях повседневного общения; обмениваться информацией, уточняя её, обращаясь за разъяснениями; выражать своё отношение к высказываемому и обсуждаемому; участвовать в полилоге, в том числе в форме дискуссии с соблюдением изучаемого языка, запрашивая и обмениваясь информацией, высказывая и аргументируя свою точку зрения; *в монологической речи:* подробно/ кратко излагать прочитанное, прослушанное, увиденное; описывать события, излагая факты; выражать свои впечатления о странах изучаемого языка и их культуре; высказывать и аргументировать свою точку зрения, делать выводы, оценивать факты /события современной жизни и культуры; *в аудировании:* отделять главную информацию от второстепенной; выявлять наиболее значимые факты, определять своё отношение к ним; извлекать из аудио текста необходимую информацию; *в чтении:* выделять необходимые факты /сведения; отделять основную информацию от второстепенной; определять временную и причинно-следственную взаимосвязь событий и явлений; обобщать описываемые факты/ явления; оценивать важность/ новизну/ достоверность информации; понимать смысл текста и его проблематик, используя элементы анализа текста; извлекать из текста лексико-грамматические явления с целью их распознания и закрепления; *в письменной речи.* излагать содержание прочитанного/ прослушанного иноязычного текста в тезисах, рефератах, обзорах; фиксировать и обобщать письменную информацию, описывать события, факты, явления.

		сообщать, запрашивать информацию, выражая собственное мнение, суждение; *в переводе.* демонстрировать умение использовать толковые и двуязычные словари и другую справочную литературу для решения переводческих задач; выполнять полный выборочный письменный перевод: с русского на английский и с английского на русский языки.
	владеть навыками /иметь опыт:	иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике и навыками устной речи; навыками реферирования, резюме, биографии на иностранном языке; навыками публичной речи, ведения дискуссии на иностранном языке.
Содержание:		Курс иностранного языка состоит из 4 основных модулей, позволяющих стандартизировать языковой материал и унифицировать требования к развитию тех или иных навыков. Языковая реализация каждого модуля предполагает тематический отбор соответствующих синтаксических структур, лексики, лингвострановедческих и экстралингвистических факторов. Каждый модуль предусматривает комплексное обучение всем видам речевой деятельности, при необходимости с усилением акцента на том или ином из них. Все модули разделены по аспектам языка и видам речевой деятельности. Основными организационными формами обучения являются: аудиторные занятия с преподавателем, текущая внеаудиторная работа студентов дома, в лингафонном кабинете, компьютерном классе, по тренировке и самоконтролю усвоения материала, самостоятельная работа студентов под руководством преподавателя как средство усиления индивидуализации. Самостоятельная работа дома предполагает такие виды работы как: подготовка к текущим практическим занятиям; внеаудиторное чтение; перевод научно-технической литературы. Самостоятельная работа в лингафонном кабинете предполагает такие виды работы как: работа с аудио/видео материалами; работа с Интернет-ресурсами. Самостоятельная работа имеет такое же методическое и материальное обеспечение, как и аудиторные занятия по иностранному языку. При определении итоговой оценки за курс иностранного языка 30% ее должна составлять оценка самостоятельной работы студентов.
Форма промежуточной аттестации:		Зачет, экзамен

Название:		Основы экономических знаний
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-2
Результаты освоения дисциплины	**знать:**	основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений; основные разделы современной экономической теории; определение экономики как науки и ее основных понятий; основные субъекты экономики; состав и содержание макроэкономических процессов;

		методы, алгоритмы и инструменты экономического анализа; способы оценки эффективности работы организации;
	уметь:	самостоятельно анализировать экономическую литературу, планировать и осуществлять свою деятельность с учетом результатов этого анализа; использовать в своей деятельности методы экономического анализа;
	владеть навыками /иметь опыт:	методами принятия экономических решений.
Содержание:		Введение в экономическую теорию. Микроэкономика. Теория потребительского поведения; Макроэкономика. История экономических учений: особенности экономических воззрений в традиционных обществах, систематизация экономических знаний, первые теоретические системы; основные этапы развития экономической теории. Формирование и эволюция современной экономической мысли. Вклад российских ученых в развитие мировой экономической мысли.
Форма промежуточной аттестации:		зачет

Название:		Правоведение
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-4
Результаты освоения дисциплины	**знать:**	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации; основные разделы современной теории права;
	уметь:	использовать в практической деятельности правовые знания; - анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, - предпринимать необходимые меры по восстановлению нарушенных прав; самостоятельно анализировать социально-политическую, юридическую литературу, планировать и осуществлять свою деятельность с учетом результатов этого анализа в рамках правового поля;
	владеть навыками /иметь опыт:	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с законодательными и нормативно-правовыми документами.
Содержание:		Предмет, метод и задачи курса “Правоведение” в вузе. Общество и государство, политическая власть. Право: понятие, нормы, отрасли. Мораль и право, правовая культура. Правоотношения и их участники. Правонарушение и юридическая ответственность. Основы конституционного строя, народовластие в Российской Федерации. Основы правового статуса человека и гражданина. Федеративное устройство России. Система органов государственной власти в России. Конституционные основы судебной системы.

	Правоохранительные органы. Основы гражданского права: гражданское правоотношение; доверенность; исковая давность; право собственности; приобретение и прекращение права собственности; защита и право собственности. Общие положения об обязательствах. Договор, понятие, форма, виды. Обязательства вследствие причинения вреда. Основы трудового права. Трудовой кодекс РФ. Социальное партнерство в сфере труда. Трудовой договор. Дисциплина труда. Дисциплинарные взыскания. Материальная ответственность сторон трудового договора. Рабочее время, время отдыха, заработная плата. Защита трудовых прав работников. Разрешение трудовых споров. Федеральная инспекция труда. Основы семейного права. Основы административного права. Основы муниципального права. Основы уголовного права. Основы экологического права и земельного законодательства. Право в сфере образовательной деятельности и культуры.
Форма промежуточной аттестации:	зачет

Название:		Основы управленческой деятельности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-6, ОПК-4, ПК-13
Результаты освоения дисциплины	**знать:**	– основные понятия и методы в области управленческой деятельности; – основные понятия и определения теории управления;
	уметь:	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; – анализировать процесс управления, выделять такие его содержательные компоненты, как разработка управленческого решения, общие функции управления, информационные и коммуникативные процессы в управлении, эффективность процесса управления и др
	владеть навыками /иметь опыт:	– навыками обоснования, выбора, реализации и контроля результатов управленческого решения – осуществлять оценку воздействия факторов внешней среды на организацию; – осуществлять оценку сильных и слабых сторон организации.
Содержание:		Сущность и методологические основы управления организацией. История развития управленческой мысли и практики. Возникновение и развитие науки управления за рубежом. Сущность и содержание теории управления. Системный подход в управлении. Организационные формы и структуры управления. Процесс управления и его содержание. Методология и организация процесса разработки управленческого решения. Общие функции управления. Информационные и коммуникативные процессы в управлении. Эффективность процесса управления. Основы теории социального управления. Человек в системе управления. Система государственного управления.
Форма промежуточной аттестации:		Зачет

Название:		Физика
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-1, ПК-11
Результаты освоения дисциплины	**знать:**	основные понятия, законы и модели механики; - основные понятия, законы и модели электричества и магнетизма; - основные понятия, законы и модели теории колебаний и волн, оптики, квантовой физики, физики твердого тела, статистической физики и термодинамики; - особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности; теоретическую часть курса на уровне, обеспечивающем ориентацию в основных принципах и направлениях развития интеллектуальных информационных,
	уметь:	– применять основные законы физики при решении прикладных задач; выбирать математические методы и реализующие их программные средства для решения конкретных задач;
	владеть навыками /иметь опыт:	навыками проведения физического эксперимента и обработки его результатов; приобрести практические умения и навыки при решении задач, сформулированных в данной рабочей программы, в различных предметных областях.
Содержание:		Физические основы механики; колебания и волны; молекулярная физика и термодинамика; электричество и магнетизм; оптика; атомная и ядерная физика; физический практикум.
Форма промежуточной аттестации:		Экзамен, зачет, зачет

Название:		Информатика
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-4
Результаты освоения дисциплины	**знать:**	основные понятия информатики. - основные понятия информатики; - формы и способы представления данных в персональном компьютере; - состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; - классификацию современных компьютерных систем; - типовые структуры и принципы организации компьютерных сетей; принципиальные основы устройства компьютера; назначение, основные функции операционных систем и средства их реализации; технологии решения задач инженерной деятельности с помощью инструментальных средств информационных технологий;

		основные понятия, принципы построения и технологию работы с базами данных; основные понятия сетей ЭВМ (локальных и глобальных), понятия сети Internet, методы поиска информации в сети Интернет; технологию создания научно-технической документации.
	уметь:	- применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); - пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; - пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; использовать программные и аппаратные средства персонального компьютера использовать полученные знания по основным функциям операционных систем для решения задач обучения, связанных с применением готовых компьютерных информационных материалов; использовать изученные инструментальные средства информационных технологий для решения практических задач инженерной деятельности; создавать и использовать несложные базы данных; искать информацию и обмениваться ею в сети Internet.
	владеть навыками /иметь опыт:	- навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); - навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией). навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.). навигацией по файловой структуре компьютера и управления файлами; технологией создания научно-технической документации различной сложности с помощью текстового процессора Microsoft Word; технологией решения типовых информационных и вычислительных задач с помощью табличного процессора Microsoft Excel; технологией решения типовых математических задач с помощью математического пакета MathCad; технологией поиска и обмена информацией в глобальных и локальных компьютерных сетях.
Содержание:		Понятие информации. Свойства информации. Данные. Операции с данными. Виды данных. Кодирование данных двоичным кодом. Таблицы кодировки ASCII. Единицы представления, измерения и хранения данных. Основные структуры данных. Предмет и задачи информатики. Основы защиты информации. Информационная безопасность и её составляющие. Угрозы безопасности информации и их классификация. Технические и программные средства реализации информационных процессов. Вычислительная техника. Компьютер. Классификация персональных компьютеров. Состав вычислительной системы (вычислительного комплекса). Текстовый редактор Microsoft Word. Понятие и основные функции текстового процессора WordМастер формул (Microsoft Equation 3.0). Электронные таблицы Microsoft Excel.
Форма промежуточной аттестации:		экзамен

Название:		Безопасность жизнедеятельности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-6
Результаты освоения дисциплины	**знать:**	основные техносферные опасности, их свойства и характеристики, характер воздействия вредных и опасных факторов на человека и природную среду, методы защиты от них применительно к сфере своей профессиональной деятельности;
	уметь:	идентифицировать основные опасности среды обитания человека, оценивать риск их реализации, выбирать методы защиты от опасностей применительно к сфере своей профессиональной деятельности и способы обеспечения комфортных условий жизнедеятельности.
	владеть навыками /иметь опыт:	законодательными и правовыми актами в области безопасности и охраны окружающей среды, требованиями к безопасности технических регламентов в сфере профессиональной деятельности; способами и технологиями защиты в чрезвычайных ситуациях; понятийно-терминологическим аппаратом в области безопасности; навыками рационализации профессиональной деятельности с целью обеспечения безопасности и защиты окружающей среды.
Содержание:		Теоретические основы БЖД. Санитарно-гигиенические основы безопасности. Промышленная безопасность. Защита населения и территории в чрезвычайных ситуациях (опасности при ЧС и защита от них).
Форма промежуточной аттестации:		зачет

Название:		Физическая культура и спорт
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-9
Результаты освоения дисциплины	**знать:**	– влияние оздоровительных систем физического воспитания на укрепление здоровья, профилактику профессиональных заболеваний и вредных привычек; – способы контроля и оценки физического развития и физической подготовленности; – правила и способы планирования индивидуальных занятий различной целевой направленности
	уметь:	– выполнять индивидуально подобные комплексы оздоровительной и адаптивной (лечебной) физической культуры, композиции ритмической и аэробной гимнастики, комплексы упражнения атлетической гимнастики; – выполнять простейшие приемы самомассажа и релаксации; преодолевать искусственные и естественные препятствия с использованием разнообразных способов передвижения; – выполнять приемы защиты и самообороны, страховки и самостраховки; – осуществлять творческое сотрудничество в коллективных формах занятий физической культурой

	владеть навыками /иметь опыт:	– средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры личности для успешной социально-культурной и профессиональной деятельности
Содержание:		Физическая культура и спорт как социальный феномен современного общества. Средства физической культуры. Основные составляющие физической культуры. Формирование физической культуры личности. Физическая культура в структуре профессионального образования. Роль отдельных систем организма в обеспечении физического развития, функциональных и двигательных возможностей организма человека. Двигательная активность и ее влияние на устойчивость, и адаптационные возможности человека к умственным и физическим нагрузкам при различных воздействиях внешней среды. Здоровье человека как ценность. Факторы его определяющие. Влияние образа жизни на здоровье. Методические принципы физического воспитания. Основы и этапы обучения движениям. Развитие физических качеств. Виды диагностики при регулярных занятиях физическими упражнениями и спортом. Самоконтроль, его основные методы, показатели. Использование отдельных методов контроля при регулярных занятиях физическими упражнениями и спортом. Методика проведения производственной гимнастики с учетом заданных условий и характера труда. Средства и методы мышечной релаксации в спорте. Оценка двигательной активности и суточных энергетических затрат. Методы самоконтроля за функциональным состоянием организма. Методы оценки уровня здоровья. Методы самоконтроля состояния здоровья, физического развития и функциональной подготовленности. Методики самостоятельного освоения отдельных элементов профессионально-прикладной физической подготовки. Методики эффективных и экономических способов овладения жизненно важными умениями и навыками
Форма промежуточной аттестации:		Зачет

Название:		Теория информации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-2, ОПК-4, ПК-7
Результаты освоения дисциплины	**знать:**	теоретические и математические основы теории информации и кодирования; различные коды и их классификацию; функциональные схемы и алгоритмы кодеров и декодеров; основные методы защиты информации.
	уметь:	находить все информационные характеристика каналов связи; строить оптимальные коды методами Шеннона-Фано и Хаффмена; кодировать методом Хемминга; строить циклические коды; строить БЧХ коды.
	владеть навыками /иметь опыт:	создания программ кодирования и декодирования на языках С++.
Содержание:		Основные понятия теории информации и теории кодирования. Энтропия вероятностной схемы. Аксиомы Хинчина и Фадеева. Условная энтропия; взаимная информация и ее свойства. Математическая модель канала связи. Пропускная способность канала

	связи. Прямая и обратная теоремы кодирования Задачи теории информации и теории кодирования. Примеры кодирования в информационных системах. Сжатие информации как кодирование. Оптимальное кодирование, префиксные коды, неравенство Крафта. Алгоритмы сжатия информации. Линейные коды, параметры кодов и их границы (граница Симмонса), корректирующие свойства кодов. Структура ЛБК. Матричное описание ЛБК. Коды Хэмминга. Расстояние Хэмминга. Геометрическая интерпретация. Границы минимального расстояния для ЛБК. Стандартное расположение. Исправление одиночной ошибки. Синдром. Совершенные и квазисовершенные коды. Простые преобразования линейного кода. Коды Рида – Маллера. Циклические коды. Код как расширение поля. Полиномиальное описание циклических кодов. Минимальные многочлены. Матричное описание циклических кодов. Коды Хэмминга как циклические. Циклические коды, исправляющие две ошибки и пакет ошибок. Коды Боуза-Чоудхури-Хоквингема. Достоинства и недостатки. Каскадные коды и коды-произведения, как развитие кодов БЧХ. Неравномерные вероятностные коды. Сверточные коды.
Форма промежуточной аттестации:	зачет

Название:		Алгебра и геометрия
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2
Результаты освоения дисциплины	**знать:**	основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями;
	уметь:	решать основные задачи векторной алгебры и аналитической геометрии; оперировать с числовыми многочленами, матрицами; решать основные задачи по теории чисел, задачи линейной алгебры, связанные с алгебраическими структурами, в том числе кольцами матриц, системами линейных уравнений над кольцами и полями, кольцами многочленов и линейными пространствами над полями; системы линейных уравнений над полями; пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; определять возможности применения теоретических положений алгебры и алгебраических методов и методов аналитической геометрии для постановки и решения конкретных прикладных задач;
	владеть навыками /иметь опыт:	методами аналитической геометрии и векторной алгебры; методами линейной.
Содержание:		Целые числа и основы теории делимости. Неопределенные уравнения I степени с двумя переменными. Основы теории сравнений. Определение и простейшие свойства сравнений. полная система вычетов по модулю.. Нормальные делители группы. Кольца, примеры колец. Основные свойства элементов кольца. Кольца вычетов. Подкольца и идеалы кольца. Поля и их простейшие свойства. Конечные поля. Подполя и расширения полей. Кольца матриц. Матрицы над кольцом и операции над ними. Общие сведения о системах линейных уравнений.. Вопросы

	делимости в кольце многочленов над полем. Неприводимые над полем многочлены. Поле разложения многочлена. Многочлены над конечными полями. Методы построения неприводимых многочленов над конечным полем Векторы и линейные операции над ними. Коллинеарные и компланарные векторы. Координаты вектора в заданном базисе. Уравнение линии на плоскости. Алгебраические линии первого и второго порядков. Уравнения прямой на плоскости. Эллипс, его уравнения и свойства. Гипербола, ее уравнение и свойства. Парабола. Уравнение параболы и основные свойства Определение, свойства векторного пространства. Конечномерные векторные пространства. Линейные преобразования векторных пространств. Собственные векторы и собственные значения линейного преобразования.
Форма промежуточной аттестации:	экзамен

	Название:	Математический анализ
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОК-8, ОПК-2
Результаты освоения дисциплины	**знать:**	основные понятия втузовского курса высшей математики: предел последовательности и функции, производная и частные производные, дифференциал, интеграл Римана от функции одной переменной, несобственные интегралы и кратные интегралы, обыкновенное дифференциальное уравнение, числовой ряд, степенной ряд, ряд Фурье; понятие векторной функции, ее производной и дифференциала, понятия скалярного и векторного полей, их основных характеристик; постановку, точные и приближенные методы решения основных задач, связанных с перечисленными выше понятиями.
	уметь:	строить графики функций в декартовой и полярной системах координат, вычислять пределы последовательностей и функций, сравнивать бесконечно малые и бесконечно большие функции; дифференцировать функции одной и нескольких переменных, заданные явно, параметрически и неявно; проводить полное их исследование с использованием методов дифференциального исчисления; вычислять неопределенные и определенные интегралы (в том числе несобственные) с помощью основных методов интегрирования и таблиц, определять сходимость несобственных интегралов, оценивать интегралы, вычислять двойные, тройные и криволинейные интегралы,
	владеть навыками /иметь опыт:	использовать интегральное исчисление при решении задач геометрии и физики; находить общие решения и решения задач Коши и некоторых краевых задач для основных классов обыкновенных дифференциальных уравнений первого и высших порядков, решать простейшие системы обыкновенных дифференциальных уравнений; определять сходимость числовых и функциональных рядов, представлять функции рядами Тейлора, проводить гармонический анализ заданных функций; переводить информацию с языка конкретной задачи на язык математических символов и строить математические модели простейших систем и процессов в естествознании и технике; классифицировать и формулировать принципы классификации.

Содержание:	Понятие функции. Обратная функция. Сложная функция. Основные элементарные функции, их свойства и графики. Элементарные функции. Параметрическое задание. Графики в полярных координатах. Предел функции в точке. Единственность предела (предельный переход в равенстве). Ограниченность функции, имеющей предел. Бесконечно малые функции. Порядковые свойства предела (предельный переход в неравенствах). Алгебраические свойства предела. Предел сложной функции (замена переменной). Односторонние пределы. Непрерывность функции в точке. Свойства функций, непрерывных в точке. Непрерывность основных элементарных функций. Свойства функций, непрерывных на отрезке: ограниченность, существование наибольшего и наименьшего значений, существование промежуточных значений. Теорема Вейерштрасса о приближении непрерывной функции многочленом. Бесконечно большие функции в точке (бесконечный предел). Классификация разрывов функции в точке. Неопределенности. Первый замечательный предел. Предел функции на бесконечности. Предел последовательности. Существование предела у монотонной ограниченной последовательности. Второй замечательный предел. Эквивалентные функции в точке и на бесконечности. Сравнение функций (символы o и O, порядок, основные эквивалентности). Понятие главной части. Свойства эквивалентных функций, применения. Производная функции в точке. Геометрический и физический смысл. Непрерывность функции, имеющей производную. Производная функция. Правила вычисления производной. Таблица производных. Производные высших порядков. Производная параметрически заданной функции. Дифференциал функции в точке как главная часть приращения. Приближенное вычисление значений функции. Касательная и нормаль к кривой. Свойства дифференциала. Инвариантность формы дифференциала (замена переменной). Дифференциалы высших порядков. Неявные функции. Теорема существования. Дифференцирование. Понятие функции нескольких переменных. График функции двух переменных. Предел и непрерывность функции двух и большего числа переменных. Двойные и повторные пределы. Свойства функций, непрерывных в точке. Свойства функций, непрерывных в замкнутой ограниченной области. Частные производные. Дифференциал. Непрерывность дифференцируемой функции. Приближенное вычисление значений функции. Касательная плоскость к поверхности. Свойства дифференциала. Инвариантность формы дифференциала. Производная по направлению. Понятие скалярного поля. Градиент. Линии или поверхности уровня. Теоремы Ферма, Ролля, Лагранжа. Следствия из теоремы Лагранжа: о нахождении интервалов монотонности, о пределе производной, об оценке погрешности вычисления значений функции. Теорема Коши. Правило Лопиталя. Шкала роста функций. Формула Тейлора для функции одной переменной. Приближенные вычисления с нужной точностью. Формулы Маклорена для основных элементарных функций. Понятие ряда Тейлора. Формула Тейлора для функции нескольких переменных с остаточным членом в форме Пеано и в форме Лагранжа. Аналог формулы Лагранжа. Исследование поведения функций одной и нескольких переменных. Монотонность, выпуклость, асимптотическое поведение. Экстремумы. Наибольшее и наименьшее значения. Условные экстремумы. Метод множителей Лагранжа. Метод наименьших квадратов. Первообразная. Неопределенный интеграл и его свойства. Методы интегрирования, использование таблиц интегралов. Основные классы функций, интегрируемых в

	элементарных функциях. Задачи, приводящие к понятию определенного интеграла. Определение интеграла. Класс интегрируемых функций. Свойства интеграла. Определенный интеграл как функция верхнего предела. Непрерывность, дифференцируемость. Формула Ньютона-Лейбница. Интегрирование по частям. Замена переменной. Предельный переход под знаком интеграла. Интегралы, зависящие от параметра. Приближенное вычисление определенного интеграла. Область определения функции. Графики элементарных функций в декартовой системе координат. Преобразование графиков. Графики функций, заданных параметрические. Графики функций в полярных координатах. Многочлены. Разложение на множители. Кратность корня. Функции. Предел функции в точке: определение и графическая интерпретация. Понятие непрерывной функции. Бесконечно малые функции. Алгебраические свойства предела. Предел сложной функции (замена переменной). Бесконечно большие функции в точке (бесконечный предел). Неопределенности. Первый замечательный предел. Односторонние пределы. Исследование функции на непрерывность. Классификация разрывов. Предел функции на бесконечности. Предел последовательности. Второй замечательный предел. Эквивалентные функции в точке и на бесконечности. Сравнение функций (символы о и О, основные эквивалентности). Понятие главной части. Вычисление пределов). Производная функции в точке. Геометрический и физический смысл. Правила вычисления производной. Таблица производных. Производные высших порядков. Производная параметрически и неявно заданной функции. Логарифмическое дифференцирование. Дифференциал функции в точке как главная часть приращения. Приближенное вычисление значений функции. Касательная и нормаль к кривой. Дифференциалы высших порядков. Физические задачи, приводящие к дифференциальным уравнениям. Дифференциальные уравнения первого порядка. Задача Коши. Теорема существования и единственности решения задачи Коши. Основные классы уравнений, интегрируемые в квадратурах. Дифференциальные уравнения, допускающие понижение порядка. Линейные дифференциальные уравнения, однородные и неоднородные. Понятие общего решения. Понижение порядка однородного линейного уравнения с помощью известного частного решения. Метод вариации постоянных. Формула Остроградского-Лиувилля для уравнений второго порядка. Линейные дифференциальные уравнения с постоянными коэффициентами. Уравнения с правой частью специального вида. Числовые ряды. Сходимость и сумма ряда. Необходимое условие сходимости. Действия с рядами. Методы исследования сходимости рядов. Степенные ряды. Интервал сходимости. Разложение функций в степенные ряды. Применение к приближенным вычислениям. Решение дифференциальных уравнений с помощью рядов. Ряды Фурье. Тригонометрическая (действительная) форма. Различные виды сходимости к функции ее ряда Фурье: в среднем квадратичном, поточечная, равномерная. Комплексная форма ряда Фурье. Понятие функции нескольких переменных. Область определения и график функции двух переменных. Предел и непрерывность функции двух переменных. Двойной и повторные пределы. Частные производные. Дифференцирование сложной функции. Дифференциал. Приближенное вычисление значений функции. Касательная плоскость к поверхности. Производная по направлению. Градиент. Линии или поверхности уровня. Частные производные и дифференциалы высших порядков. Неявные функции. Теорема существования.

	Дифференцирование. Правило Лопиталя. Шкала роста функций. Формула Тейлора для функции одной переменной с остаточным членом в форме Пеано и в форме Лагранжа. Приближенные вычисления с нужной точностью. Формула Тейлора для функции нескольких переменных. Исследование поведения функций одной и нескольких переменных. Монотонность, выпуклость, асимптотическое поведение. Экстремумы. Наибольшее и наименьшее значения. Условные экстремумы. Метод множителей Лагранжа. Нахождение неопределенного интеграла с использованием таблиц интегралов и свойств линейности и инвариантности интегральных формул. Метод интегрирования по частям. Интегрирование рациональных функций. Метод замены переменной. Вычисление определенного интеграла. Интегрирование по частям, замена переменной.
Форма промежуточной аттестации:	Экзамен, зачет

Название:		Дискретная математика
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2
Результаты освоения дисциплины	**знать:**	– аппарат алгебры логики и теорию булевых функций; – основы теории множеств; – логику бинарных отношений и предикатов; – теорию отображений и алгебру подстановок; – основы алгебры вычетов;
	уметь:	– строить таблицы истинности для формул логики и упрощать формулы логики; – представлять булевы функции в виде формул заданного типа, проверять множество булевых функций на полноту; – выполнять операции над множествами применять аппарат теории множеств для решения задач; – выполнять операции над предикатами, записывать области истинности предикатов, формализовать предложения с помощью логики предикатов; – исследовать бинарные отношения на заданные свойства;
	владеть навыками /иметь опыт:	– выполнять операции над отображениями и подстановками, выделять структурные особенности отображений и подстановок; – выполнять операции в алгебре вычетов; – строить автоматы с заданными свойствами
Содержание:		Алгебра логики. Функции алгебры логики. Формулы. Реализация функций формулами, эквивалентность формул. Свойства элементарных функций. Принцип двойственности. Разложение функций алгебры логики по переменным. Совершенная дизъюнктивная нормальная форма. Полнота и замкнутость, примеры полных систем. Важнейшие замкнутые классы, теорема о полноте. Представление о результатах Поста. Ограниченно-детерминированные (автоматные) функции. Диаграммы переходов. Канонические уравнения. Операции над ограниченно-детерминированными функциями. Примеры полных систем. Пример универсальной ограниченно-детерминированной функции. Проблема распознавания полноты систем ограниченно-детерминированных

	функций.
Форма промежуточной аттестации:	Экзамен

Название:		Теория вероятностей и математическая статистика
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2
Результаты освоения дисциплины	**знать:**	– теоретическую часть курса на уровне, обеспечивающем ориентацию в основных принципах и направлениях развития интеллектуальных информационных,
	уметь:	– выбирать математические методы и реализующие их программные средства для решения конкретных задач;
	владеть навыками /иметь опыт:	– приобрести практические умения и навыки при решении задач, сформулированных в данной рабочей программы, в различных предметных областях.
Содержание:		Основы теории вероятностей Случайные величины. Распределение вероятностей Последовательности случайных величин. Аналитические методы в теории вероятностей Основы теории случайных процессов
Форма промежуточной аттестации:		Экзамен

Название:		Информационные технологии
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-4, ПК-6, ПСК-1.3
Результаты освоения дисциплины	**знать:**	– основные принципы, методы и свойства информационных и телекоммуникационных технологий в профессиональной деятельности. – основы эксплуатации и безопасности операционных систем; – основы технологий виртуализации; – основы защиты данных в сети; – основы СУБД; – методы проектирования, планирования и моделирования в предметной области с использованием информационных технологий; – основы работы поисковых систем в Интернет, принципы построения web-приложений. – методы обработки данных, реализованные в информационно-аналитических системах поддержки принятия решений.
	уметь:	– получать информацию в локальных и глобальных компьютерных сетях; – применять графические редакторы для создания и редактирования изображений; – применять компьютерные программы для поиска информации, составления и оформления документов и презентаций;

		– использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах; – обрабатывать и анализировать информацию с применением программных средств и вычислительной техники;
	владеть навыками /иметь опыт:	– навыками самостоятельного поиска и усвоения новых знаний в данной области; – принципами выбора информационных систем для решения типовых профессиональных задач.
Содержание:		1 Понятие информации и информационных технологий. Операционные системы, технологии защиты данных в них, ОС с открытым кодом. Виртуальные машины. Подготовка различного рода проектной документации в предметной области с применением MS Visio. Изучение возможностей по управлению проектами и ресурсами в организациях с помощью современных информационных технологий, MS Project. 2 Основные редакторы MicrosoftOffice, средства обработки и защиты данных в них. Пароли, цифровая подпись. Основы баз данных. Проектирование базы данных и обработка данных в Access. Шифрование, разграничение доступа, пароли, резервирование. Системы моделирования и аналитической поддержки. Функции и возможности систем Arena, Mathcad, Deductor. Основы использования компьютерных сетей. Локальные и глобальные компьютерные сети. Технология поиска информации в Internet. Поисковые системы в Интернет.Основные протоколы Internet.Основы web-технологий. Защита электронной почты и браузеров. Антивирусы. Снифферы. Системы анализа рисков.
Форма промежуточной аттестации:		Экзамен

Название:		Математический аппарат и средства анализа безопасности программного обеспечения
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-2, ПК-2, ПСК-1.4
Результаты освоения дисциплины	**знать:**	- методы и средства анализа ПО; - основы построения защищенных ПО.
	Уметь:	- пользоваться средствами анализа безопасности ПО; - анализировать и оценивать угрозы информационной безопасности ПО.
	владеть навыками /иметь опыт:	- методами и средствами анализа безопасности ПО; - разработка безопасного ПО.
Содержание:		Модели угроз безопасности программного продукта. Количественные и качественные метрики оценивания качества ПО. Оценка надежности ПО. Основные ошибки программистов при написании кода, их методы и способы обнаружения. Средства анализа безопасности ПО.
Форма промежуточной аттестации:		Зачет с оценкой

Название:		Электроника и схемотехника
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-3
Результаты освоения дисциплины	**знать:**	принципы работы полупроводниковых приборов; принцип работы операционных усилителей; основные принципы построения усилительных каскадов на биполярных и полевых транзисторах; принципы функционирования нелинейных и функциональных преобразователей; принципы построения устройств на операционных усилителях; принципы построения источников вторичного электропитания; принципы работы аналоговых и цифровых ключей и коммутаторов; принципы построения базовых логических элементов
	уметь:	решать задачи по курсу «Электроника»; производить расчеты усилительных каскадов на биполярных и полевых транзисторах;
	владеть навыками /иметь опыт:	производить расчеты схем на операционных усилителях; производить расчеты схем источников вторичного электропитания
Содержание:		Определение, классификация и области применения аналоговых, и цифровых электронных устройств. Аналоговая и цифровая формы представления сигналов. Общие сведения об аналоговых электронных устройствах. Основные определения. Классификация. Основные технические показатели и характеристики.. Влияние ОС на параметры и характеристики усилителя. Устойчивость усилителей, охваченных отрицательной ОС. Применение операционных усилителей. Операционные усилители, их основные характеристики. Типовые схемы включения ОУ, нелинейные преобразователи на ОУ. Особенности и назначение активных фильтров. Активные фильтры на операционных усилителях. Генераторы электрических колебаний. Назначение и виды генераторов. Принципы построения. Генераторы гармонических сигналов. Кварцевые генераторы. Источники питания электронных устройств. Принципы построения вторичных источников питания. Выпрямители источников электропитания. Стабилизаторы напряжения. Импульсные источники вторичного электропитания.
Форма промежуточной аттестации:		Экзамен

Название:		Языки программирования
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-4, ПК-2, ПСК-1.3
Результаты освоения дисциплины	**знать:**	– основные способы представления данных и приемы алгоритмизации; – основные этапы решения задач на компьютере; – основные методы и средства разработки корректных алгоритмов и программ; – правила и приемы при программировании типовых задач; способы записи и документирования алгоритмов и программ; – способы испытания и отладки программ; – основные понятия и методы технологии программирования, в

		том числе структурного и объектно-ориентированного подхода; – конструкции языка С++
	уметь:	– формализовать поставленную задачу; – применять полученные знания для решения задач автоматизации в различных предметных областях; – составлять и оформлять программы на языке программирования С++; – тестировать и отлаживать программы; – работать с ресурсами компьютера программными средствами
	владеть навыками /иметь опыт:	– навыками работы с современными интегрированными средами разработки программного обеспечения; – навыками разработки алгоритмов решения прикладных задач и реализации их в виде программ на языке высокого уровня.
Содержание:		1.Основы программирования на языках высокого уровня Структурное программирование 2.1.Разветвляющиеся вычислительные процессы. 2.2. Циклические вычислительные процессы. Модульное программирование 3.1. Проектирование программных алгоритмов (основные принципы и подходы). 3.2. Пользовательские функции. 3.3. Рекурсия и итерация. Типизация и структуризация программных данных. 4.1. Группы данных (вектор). 4.2. Группы данных (массив фиксированного размера). 4.3. Обработка текстовой информации в С++. 4.4. Структуры. Ввод-вывод в С++ 5.1. Потоки 5.2. Файлы. Статические и динамические данные Сложные структуры данных (списки, деревья, сети) Сортировки Методы и средства объектно-ориентированного программирования Обработка исключительных ситуаций Макропроцессоры, макрогенераторы Язык Ассемблера
Форма промежуточной аттестации:		Зачет, экзамен

Название:		Основы информационной безопасности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-5, ОПК-7, ПСК-1.1
Результаты освоения дисциплины	**знать:**	– цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; – методологию создания систем защиты информации; – направления развития средств и методов обеспечения информационной безопасности; – роль и место информационной безопасности в системе национальной безопасности; – угрозы информационной безопасности государства;

		– содержание информационной войны, средств и методов ее ведения; – современные подходы к построению систем защиты информации; – компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения информационной безопасности;
	уметь:	– выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; – применять полученные знания при выполнении курсовых и дипломных работ и проектов, а также в ходе научных исследований
	владеть навыками /иметь опыт:	– навыками формальной постановки и решения задач обеспечения информационной безопасности компьютерных систем.
Содержание:		Понятие национальной безопасности. Виды безопасности в жизнедеятельности личности, общества, государства. Место информационной безопасности (ИБ) в системе национальной безопасности РФ. Основные составляющие национальных интересов Российской Федерации (РФ) в информационной сфере. Интересы личности, общества, государства. Государственная информационная политика. Виды угроз информационной безопасности РФ. Анализ угроз ИБ. Объекты защиты информации. Источники угроз информационной безопасности РФ. Внешние и внутренние угрозы. Требования по информационной безопасности. Проблемы региональной информационной безопасности. Показатели информационной безопасности. Информационная война, информационное противоборство и информационная безопасность: субъекты, цели, методы. Проблемы информационных воин. Информационное оружие, его классификация и возможности. Модели саморазвивающихся систем и их использование для анализа проблем информационного противоборства. Основные понятия и общеметодологические теории обеспечения информационной безопасности. Классификация свойств и показателей информации по требованиям информационной безопасности. Виды информации. Классификация угроз информационной безопасности, анализ угроз ИБ, проблемы информационной войны Государственная информационная политика. Требования к обеспечению информационной безопасности. Проблемы региональной информационной безопасности. Условия функционирования систем защиты информации. Методы и средства обеспечения информационной безопасности. Классификация средств обеспечения информационной безопасности. Виды информации. Методы нарушения конфиденциальности, целостности и доступности. Причины, виды, каналы утечки и искажения информации. Компьютерная система как объект информационной безопасности: структура, объекты защиты. Общая характеристика средств и методов обеспечения информационной безопасности в компьютерных системах.
Форма промежуточной аттестации:		Экзамен

Название:	Гуманитарные аспекты информационной безопасности
Название и номер направления и/или специальности:	10.03.01 Информационная безопасность

Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-5, ОК-6, ОПК-4
Результаты освоения дисциплины	**знать:**	– социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; – способы работы в коллективе, толерантно воспринимая социальные, культурные и иные различия; – значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	уметь:	– понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; – работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; – понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	владеть навыками/ иметь опыт:	– понимания социальной значимости своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; – работы в коллективе, толерантно воспринимая социальные, культурные и иные различия; – понимания значения информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
Содержание:		Гуманитарные аспекты информационной безопасности и понятие о функциях языка, видах и особенностях мышления Базовые понятия системной логики, системно-логические операции Информационное воздействие на человека и манипуляция сознанием Основы теории информационно-психологического воздействия
Форма промежуточной аттестации:		Зачет

Название:		Технологии и методы программирования
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-4, ПК-2
Результаты освоения дисциплины	**знать:**	– методологию построения алгоритмов и порождаемых ими вычислительных процессов; – основные парадигмы программирования; – конструктивные компоненты и структуру компьютерных программ; – основные конструкции языка программирования высокого уровня;

	уметь:	– поэтапно проводить разработку программного обеспечения; – разрабатывать качественное программного обеспечения; – использовать модульный подход разработки программного обеспечения; – использовать различные методы проектирования программного обеспечения; – разрабатывать программную документацию; – анализировать и обобщать воспринимаемую информацию; – находить ошибки в программе и исправлять их; – самостоятельно работать с технической и справочной литературой;
	владеть навыками /иметь опыт:	– навыками применения современных технологий программирования при разработке программного обеспечения; – современными техническими и программными способами взаимодействия пользователя с ЭВМ;
Содержание:		Модуль 1. Алгоритмы и структуры данных: Абстракции данных (реализация абстрактного списка при помощи связного списка и динамического массива). Алгоритмы сортировки и поиска. Модели вычислений. Машина Тьюринга. Оценка эффективности алгоритмов. Алгоритмы на графах. Модуль 2. Технология программирования. Основы. Жизненный цикл ПО. Анализ требований. Модуль 3. Основы ООП. Объектно-информационные- модели. Язык C++. Классы и объекты, поля и методы, инкапсуляция. Конструкторы и деструкторы. Шаблоны. Исключения. Модуль 4. Современные технологии программирования. ООП. Архитектура .NET. Язык C#. Наследование и полиморфизм. Интерфейсов базовой библиотеки классов .NET Модуль 5. Современные технологии программирования. ООП. Основы разработки визуального интерфейса. Язык C#. Модуль 6. Современные технологии программирования. ООП. Проектирование ПО. Модуль 7. Современные технологии программирования. Тестирование ПО.
Форма промежуточной аттестации:		Зачет, экзамен

Название:		Криптографические методы защиты информации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2, ПК-1
Результаты освоения дисциплины	**знать:**	– основы системного подхода к организации защиты информации, передаваемой, обрабатываемой и хранимой техническими средствами на основе применения криптографических методов; – основные принципы проектирования и анализа шифров; – основы математических методов, которые используются при проектировании и анализе шифров.
	уметь:	– оценивать сложность алгоритмов криптографии и их криптостойкость; – классифицировать шифры.

	владеть навыками /иметь опыт:	– владеть навыками шифрования и дешифрования текста, используя различные шифры;
Содержание:		Введение. Криптография как механизм защиты. Традиционные симметричные шифры. Современные симметричные шифры. Алгоритмы распределения ключей. Асимметричные криптосистемы. Однонаправленные ХЭШ-функции. Коды аутентификации сообщений-(MAC). ЭЦП (электронно-цифровая подпись). Создание случайных чисел. Протоколы аутентификации.
Форма промежуточной аттестации:		Экзамен

Название:		Техническая защиты информации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-1, ПК-1, ПК-6
Результаты освоения дисциплины	**знать:**	виды, источники и носители защищаемой информации, основные угрозы безопасности информации, концепцию инженерно-технической защиты информации, основные принципы и методы защиты информации, основные руководящие и нормативные документы по инженерно-технической защите информации, порядок организации инженерно-технической защиты информации;
	уметь:	выявлять угрозы и технические каналы утечки информации, описывать объекты защиты и угрозы безопасности информации, применять наиболее эффективные методы и средства инженерно-технической защиты информации, контролировать эффективность мер защиты;
	владеть навыками /иметь опыт:	навыками аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем, инженерного расчета размеров контролируемой зоны
Содержание:		Концепция инженерно-технической защиты информации. Системный подход к защите информации. Основные концептуальные положения инженерно-технической защиты информации. Теоретические основы инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов защиты Модели злоумышленника. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Технические каналы утечки информации. Физические основы защиты информации. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные направления развития технической разведки. Средства технической разведки. Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Государственная система защиты информации. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств. Контроль эффективности инженерно-технической защиты

	информации.
Форма промежуточной аттестации:	Экзамен

Название:		Организационное и правовое обеспечение информационной безопасности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-4, ОПК-5, ПК-8, ПК-15
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 в ТКС.
Форма промежуточной аттестации:		Зачет

Название:		Программно-аппаратные средства защиты информации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-7, ПК-1, ПК-6
Результаты освоения дисциплины	**знать:**	– методологические и технологические основы обеспечения информационной безопасности сетевых автоматизированных систем; – угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем; – типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения; – роль человеческого фактора в обеспечении безопасности сетей; – возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях; – принципы функционирования основных защищенных сетевых протоколов; – основы применения межсетевых экранов для защиты сетей; – правила определение политики сетевой безопасности; – стандарты по оценке защищенных сетевых систем и их теоретические основы; – методы и средства проектирования, реализации и оценки защищенных сетевых систем;
	уметь:	– проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности; – разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы и средства и теоретические основы; – применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации в автоматизированных системах; – применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты информации в сетях; – реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения; – реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем;
	владеть навыками /иметь опыт:	– умением пользоваться системами анализа защищенности
Содержание:		Основные понятия и содержание дисциплины; Основные подходы к защите данных от несанкционированного доступа; Программно-аппаратные средства шифрования; Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям; Защита программ с использованием аппаратных ключей; Надежность систем ограничения доступа; Защита от разрушающих программных воздействий; Системные вопросы защиты программ и данных; Обеспечение безопасности ОС Linux.
Форма промежуточной аттестации:		Экзамен, курсовой проект

Название:		Основы управления информационной безопасностью
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-7, ПК-10, ПК-13
Результаты освоения дисциплины	**знать:**	– методы и средства управления информационной безопасностью;
	уметь:	– инфраструктурой; – 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 работы с нормативной документацией по обеспечению информационной безопасности; – навыками 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. Классификация ресурсов и их контроль. Ответственность за ресурсы. Классификация информации Безопасность персонала. Безопасность в должностных инструкциях и при выделении ресурсов. Администрирование компьютерных систем и вычислительный 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 Вопросы бесперебойной работы организации. Выполнение требований. Выполнение правовых требований. Проверка безопасности информационных систем. Аудит систем.
Форма промежуточной аттестации:		Экзамен

Название:		Основы деловой и научной коммуникации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-7, ОПК-4, ПК-8, ПК-9
Результаты освоения дисциплины	**знать:**	основы владения правилами и нормами современного русского литературного языка и культуры речи, риторики/практической риторики, теории коммуникации, делового общения, этики деловой коммуникации;
	уметь:	общаться, вести гармонический диалог и добиваться успеха в процессе коммуникации; использовать полученные общие знания в

		профессиональной деятельности; строить устную и письменную речь, опираясь на законы логики, аргументировано и ясно излагать собственное мнение; грамотно строить коммуникацию в конфликтных ситуациях.
	владеть навыками /иметь опыт:	коммуникативными навыками в разных сферах употребления национального языка, письменной и устной его разновидностей.
Содержание:		Русский литературный язык как основа изучения культуры речи. Функциональные стили русского литературного языка. Культура речи и ее значение в жизни общества. Языковая норма. Типы норм: орфоэпические, акцентологические, лексические, грамматические, стилистические. Нормы правописания и пунктуационные нормы. Речевое взаимодействие. Коммуникативные качества речи.
Форма промежуточной аттестации:		зачет

Название:		Математическая логика и теория алгоритмов
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2
Результаты освоения дисциплины	**знать:**	– основы исчисления высказываний; – основы исчисления предикатов; – основные подходы к формализации понятия алгоритма;
	уметь:	– применять логические и алгоритмические методы в криптографии; – оценивать сложности алгоритмов и методах построения эффективных алгоритмов;
	владеть навыками /иметь опыт:	– оценивать сложность алгоритмов и вычислений; – классифицировать алгоритмы по классам сложности.
Содержание:		Логика высказываний. Логические связки. Формулы алгебры высказываний. Тождественно-истинные формулы. Равносильность формул. Логическое следование. Представление булевых функций формулами Замкнутые классы. Критерии полноты систем булевых функций. Псевдобулевы функции и их представление рядами Фурье. Представление функций многозначной логики рядами Фурье. Минимизация булевых функций. Классификация функций К-значной логики, системы функций К-значной логики, критерии полноты систем функций К-значной логики. Особенности k-значных логик. Исчисления высказываний и предикатов, их полнота и непротиворечивость. Аксиоматические системы, формальный вывод. Вывод из семейства гипотез. Свойства. Непротиворечивость и полнота исчисления высказываний. Независимость системы аксиом исчисления высказываний. Примеры аксиоматизаций исчисления высказываний. Реляционная алгебра и реляционное исчисление. Предикаты. Операции над предикатами. Теория алгоритмов. Алгоритмически разрешимые и неразрешимые проблемы. Нормальные алгоритмы. Понятие о сложности алгоритмов. Подходы к оценкам сложности алгоритмов. Комбинационная сложность схем.
Форма промежуточной аттестации:		Экзамен

Название:		Социология организаций и организационное поведение
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-6 ОПК-4 ПК-14
Результаты освоения дисциплины	**знать:**	– основы исчисления высказываний; – основы исчисления предикатов; – основные подходы к формализации понятия алгоритма;
	уметь:	– применять логические и алгоритмические методы в криптографии; – оценивать сложности алгоритмов и методах построения эффективных алгоритмов;
	владеть навыками /иметь опыт:	– оценивать сложность алгоритмов и вычислений; – классифицировать алгоритмы по классам сложности.
Содержание:		Логика высказываний. Логические связки. Формулы алгебры высказываний. Тождественно-истинные формулы. Равносильность формул. Логическое следование. Представление булевых функций формулами Замкнутые классы. Критерии полноты систем булевых функций. Псевдобулевы функции и их представление рядами Фурье. Представление функций многозначной логики рядами Фурье. Минимизация булевых функций. Классификация функций К-значной логики, системы функций К-значной логики, критерии полноты систем функций К-значной логики. Особенности k-значных логик. Исчисления высказываний и предикатов, их полнота и непротиворечивость. Аксиоматические системы, формальный вывод. Вывод из семейства гипотез. Свойства. Непротиворечивость и полнота исчисления высказываний. Независимость системы аксиом исчисления высказываний. Примеры аксиоматизаций исчисления высказываний. Реляционная алгебра и реляционное исчисление. Предикаты. Операции над предикатами. Теория алгоритмов. Алгоритмически разрешимые и неразрешимые проблемы. Нормальные алгоритмы. Понятие о сложности алгоритмов. Подходы к оценкам сложности алгоритмов. Комбинационная сложность схем.
Форма промежуточной аттестации:		Зачет

Название:		Защита информации в процессе документооборота организации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОПК-7, ПК-8, ПК-13
Результаты освоения дисциплины	**знать:**	– теоретические и методические основы рационального построения защищенного документооборота в любых организационных структурах; – функциональные возможности и предпосылки безопасного применения различных типов технологических систем и способов обработки и хранения документов; – принципы и методы безопасной обработки электронных документов в потоках при любых используемых типах систем и способах выполнения процедур и операций по обработке и хранению этих документов;

		– методы и средства защиты электронной документированной информации и носителя этой информации от несанкционированного доступа в процессе выполнения каждой процедуры и операции; – современные системы электронного документооборота отечественного и зарубежного производства, основные функции и возможности СЭД по защите информации; – профессиональный уровень организации защищенного делопроизводства в офисе с целью эффективного и безопасного информационно-документационного обеспечения управления фирмой.
	уметь:	– оформлять различные документы с учетом требований ГОСТ Р 6.30-2003; – разрабатывать основные положения концепции применения комплексных систем защиты информации в автоматизированных системах; – разрабатывать организационно-распорядительные документы по вопросам защиты информации; – ориентироваться в средствах защиты информации от несанкционированного доступа; – обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации в автоматизированных системах.
	владеть навыками /иметь опыт:	– навыками безопасной работы с документами на основе технологий электронного документооборота, – приемами защиты документооборота, обеспечения безопасности процессов составления и ввода электронных документов, их хранения, передачи, обработки, систематизации. – навыками планирования защищенного документооборота бизнес-процессов, контроля исполнения.
Содержание:		Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Государственная тайна. Персональные данные. Различные виды тайн. Документирование конфиденциальной информации. Особенности документирования конфиденциальной информации Специфика оформления реквизитов конфиденциальных документов. Специфика оформления реквизитов конфиденциальных документов. Организация конфиденциального документооборота. Особенности учета и регистрации конфиденциальной документированной информации. Обработка входящих, внутренних и исходящих конфиденциальных документов, их учет и регистрация. Разрешительная система доступа к конфиденциальной информации. Общие сведения. Регламент доступа к конфиденциальным документам. Экспертная комиссия по защите конфиденциальной информации. Особенности доступа к архивным конфиденциальным документам. Составление номенклатуры дел, формирование и оформление конфиденциальных дел. Особенности учета конфиденциальных дел и составления номенклатуры конфиденциальных дел. Формирование. Архивного хранения конфиденциальных документов и дел и уничтожение. Экспертиза ценности конфиденциальных документов. Подготовка конфиденциальных документов и дел для архивного хранения. Подготовка конфиденциальных документов и дел к уничтожению.. Оформление конфиденциальных дел. Режим конфиденциальности документированной информации. Режим обмена конфиденциальной документированной информацией. Требования к сотрудникам, работающим с конфиденциальной информацией. Режим сохранности конфиденциальных документов и дел. Режим конфиденциальности при проведении совещаний и переговоров. Проверка наличия

	носителей конфиденциальной информации.. Система защищенного электронного документооборота. Особенности конфиденциального электронного документооборота. ИБ при осуществлении МЭД и ВЭД обеспечивается комплексом технических и организационных мероприятий. Основные задачи обеспечения защиты информации, циркулирующей в АИС, и самих систем на уровне единой информационной среды организации. Основные виды угроз информационной безопасности организации. Основные требования по защите конфиденциальной информации. Защита системы электронных сообщений. Общие требования для задач, связанных с контролем почтового трафика.
Форма промежуточной аттестации:	Экзамен

	Название:	Аппаратные средства вычислительной техники
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОПК-3, ПК-6, ПСК-1.2
Результаты освоения дисциплины	**знать:**	– историю развития, состояние и тенденции развития вычислительной техники; – классификацию вычислительных машин и основные характеристики различных классов ЭВМ; – архитектуру, принципы построения и работы ЭВМ и их основных узлов; – архитектуру и возможности микропроцессорных комплектов; – принципы построения и работы ПЭВМ; – аппаратно-программные средства диагностики ПЭВМ.
	уметь:	– использовать программные и аппаратные средства персонального компьютера
	владеть навыками /иметь опыт:	– навыками чтения электронных схем; – профессиональной терминологией; – навыками безопасного использования технических средств в профессиональной деятельности.
	Содержание:	Устройства с памятью. Организация процессора и основной памяти. Построение преобразователей информации и устройств с памятью. Типовые узлы ЭВМ. Организация взаимодействия основных устройств ЭВМ. Характеристика интерфейса периферийных устройств. Периферийные устройства ЭВМ Микропроцессоры Архитектура и структурное построение. Микропроцессорные системы. Архитектура и принципы работы ПЭВМ ПЭВМ. Архитектура современных ПЭВМ. Системная плата, ее назначение, основные элементы и их взаимодействие в системе. Системная бакалавраль. Основные стандарты системных бакалавралей (шин). Буферизация шин. Управление системной бакалавралью. Адаптеры внешних устройств (платы расширения). ПЭВМ, рабочие станции и серверы Использование ПЭВМ в системе обработки информации. ПЭВМ, АРМ, средства обработки сигналов на базе ПЭВМ, архитектура

	рабочих станций и серверов. Итоги изучения дисциплины.
Форма промежуточной аттестации:	Зачет

	Название:	Защита информации в предпринимательской деятельности
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОПК-4, ПК-7, ПК-13
Результаты освоения дисциплины	**знать:**	– виды, источники и носители защищаемой коммерческой информации; – основные угрозы безопасности информации в процессе ПД; – концепцию организационной и программно-технической защиты информации в ПД; – основные принципы и методы защиты коммерческой информации; – основные руководящие и нормативные документы по защите информации в процессе ПД; – порядок организации защиты информации в ПД.
	уметь:	– выявлять угрозы и технические каналы утечки коммерческой информации; – описывать (моделировать) объекты защиты и угрозы безопасности информации в процессе ПД; – применять наиболее эффективные методы и средства защиты информации в процессе ПД; – контролировать эффективность мер защиты.
	владеть навыками /иметь опыт:	– навыками работы со средствами защиты коммерческой информации; – навыками оценки эффективности мер защиты информации в процессе ПД.
	Содержание:	Информация в предпринимательской деятельности Принципы и методы защиты коммерческой информации Минимизация предпринимательского риска Обеспечение защиты интеллектуальной собственности Особенности защиты информации в чрезвычайных ситуациях Организация и экономика защиты информации на предприятиях
	Форма промежуточной аттестации:	Зачет с оценкой

Название:		Сети и системы передачи информации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-4, ПК-2
Результаты освоения дисциплины	**знать:**	– основные понятия построения систем и сетей электросвязи и особенности их эксплуатации; – тактико-технические характеристики основных телекоммуникационных систем сигналов и протоколов, применяемых для передачи различных видов сообщений; – перспективы развития систем и сетей связи;
	уметь:	– творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; – отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; – разрабатывать структурные схемы систем связи с заданными характеристиками; – читать структурные и функциональные схемы систем и сетей связи
	владеть навыками /иметь опыт:	– анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; анализа сетевых протоколов; – работы с научно-технической литературой по изучению перспективных систем и сетей связи с целью повышения эффективности использования защищенных телекоммуникационных систем
Содержание:		Объект и предмет изучения. Базовые понятия и определения. Краткая справка о развитии систем электрической связи и научных достижениях. Классификация систем связи. Каналы, системы и сети электрической связи. Обобщенная модель информационных систем. Сигналы и их представление. Кодирование информации в системах связи: помехоустойчивое кодирование; схемная реализация; алгоритмы декодирования. Методы модуляции при передаче непрерывных сообщений: основные типы модемов; уплотнение информации в системах связи. Цифровые методы передачи непрерывных сообщений. Особенности передачи дискретных сообщений по цифровым каналам. Цифровая обработка аналоговых сигналов. Дискретные вокодеры. Основы теории многоканальной электросвязи. Особенности цифровых систем многоканальных передач сообщений. Способы объединения цифровых потоков. Кабельные и волноводные системы связи: системы телефонной связи; цифровая телефония; системы телеграфной связи; коротковолновые и ультракоротковолновые системы связи; радиорелейные системы связи; телевизионные системы; спутниковые системы связи; волоконно-оптические системы связи; современные виды информационного обслуживания; факсимильная передача информации; электронная почта; телеконференция; видеотекс; телетекст; сети связи. Структура, характеристики и многоуровневая организация управления в ИВС: структура; характеристики ИВС; процессы; многоуровневая организация управления ИВС; интерфейсы; структура сообщений; протоколы; распределение функций по системам. Структура сетей связи. Методы коммутации информации. Особенности сетей с

	коммутацией каналов, сообщений и пакетов. Адресация, маршрутизация пакетов и управление потоками: способы адресации; маршрутизация пакетов; Управление потоками; защита от перегрузок. Эталонная модель взаимодействия открытых систем. Общие сведения о протоколах эталонной семиуровневой модели. Протоколы физического уровня; интерфейс X.21; протоколы канального уровня; протокол X.25. Глобальные и локальные сети: особенности современных сетевых архитектур; архитектурные особенности современных локальных сетей. Технические характеристики и принципы функционирования современных модемов. Сети интегрального обслуживания. Синтез глобальной сети радиальной структуры. Синтез глобальной сети древовидной структуры. Синтез глобальной распределенной сети. Изучение работы звена связи вычислительной сети в протоколе HDLC (канальный уровень). Маршрутизация пакетов. Маршрутизация пакетов и управление потоком сообщений с помощью окна. Кольцевые локальные вычислительные сети (Cambridge Ring). Локальная вычислительная сеть Ethernet. Основы моделирования в пакете MatLab 5.x. Спектральный анализ сигналов. Исследование характеристик цифровых фильтров. Синтез цифровых БИХ- и КИХ-фильтров. Модуляция сигнала
Форма промежуточной аттестации:	экзамен

	Название:	История становления систем информационной безопасности
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ОК-3, ОК-5, ОПК-4
Результаты освоения дисциплины	**знать:**	О критериях, которым должно соответствовать информационное общество, о соответствии современного общества этим критериям. Знать периоды развития информационной безопасности, этапы развития вычислительной техники, критерии периодизации, развитие элементной базы, ведущих ученых в этой области, развитие отечественной вычислительной техники и информационной безопасности в России.
	уметь:	Уметь осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики.
	владеть навыками /иметь опыт:	Проводить поиск информации по требуемой тематике, аргументировано и последовательно излагать свое мнение, проводить сравнительный анализ состояния общества и вычислительной техники. Обладать способностью к логически правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.
	Содержание:	Понятие об информационной безопасности. Основные термины и определения. Шифрование. Дешифрование. Понятие ключа к шифру. Многоалфавитный шифр. Криптографическая деятельность при Петре 1 Российский «черный кабинет» против внешних и внутренних

	врагов.Способы шифрования информации. Вклад в шифрование Эйлера и Альберти. Шифр «Цифирь». Шифр Де Ла Порта. Криптографическая деятельность организаций «Земля и воля» и «Народная воля» в России в 1876–1881 годах. Работа Охранного отделения. Способы повышения криптостойкости шифра. Криптография во время гражданской войны. Способы шифрования информации. Работа «цифирного отделения». Начало радиовойны в эфире. Радиоразведка Русского Императорского Флота на Балтийском море: история создания. Становление Службы Информационной Безопасности в СССР. Диаграмматические шифры – шаг к современной стеганографии. Криптографический фронт Великой Отечественной войны. Шифровальная машина «Энигма». Операция по дешифрованию «Ультра»/ Шифр «Система измененных знаков» Вклад А. С. Попова в историю отечественной радиоразведки. Радиосвязь в СССР и радиотехнические службы органов безопасности в первой половине XX века История цифровых систем засекречивания речевого сигнала. Побочные электромагнитные излучения электронной вычислительной техники и их маскировка. Особенности Российской шифровальной и дешифровальной службы.
Форма промежуточной аттестации:	Зачет

Название:		Иностранный язык (технический перевод)
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-7, ОПК-4, ПК-9
,Результаты освоения дисциплины	**знать:**	– значение новых лексических единиц, связанных с тематикой данного этапа обучения и соответствующими ситуациями общения, в том числе оценочной лексики, реплик-клише речевого этикета, отражающих особенности культуры стран изучаемого языка; – этапы процесса развития вычислительных систем и информационных технологий; – значение изученных грамматических явлений (видовременные, неличные и неопределённо-личные формы глагола, формы условного наклонения, косвенная речь (косвенные вопросы), согласование времён и др.); – особенности разговорного, литературного, профессионально-делового и публицистического стилей; – страноведческую информацию из аутентичных источников. Сведения о стране/ странах изучаемого языка, их науке и культуре, исторических и современных реалиях, общественных деятелях, месте в мировом сообществе и мировой культуре.
	уметь:	– использовать знания иностранного языка в профессиональной деятельности и межличностном общении; – читать и переводить тексты общей, общетехнической, профессиональной направленности;

		• *в диалогической речи:* – участвовать в разговоре, беседе в ситуациях повседневного общения; – обмениваться информацией, уточняя её, обращаясь за разъяснениями; – выражать своё отношение к высказываемому и обсуждаемому; – участвовать в полилоге, в том числе в форме дискуссии с соблюдением изучаемого языка, запрашивая и обмениваясь информацией, высказывая и аргументируя свою точку зрения; • *в монологической речи:* – подробно/ кратко излагать прочитанное, прослушанное, увиденное; – описывать события, излагая факты; – выражать свои впечатления о странах изучаемого языка и их культуре; – высказывать и аргументировать свою точку зрения, делать выводы, оценивать факты /события современной жизни и культуры; • *в аудировании:* – отделять главную информацию от второстепенной; – выявлять наиболее значимые факты, определять своё отношение к ним; – извлекать из аудио текста необходимую информацию; • *в чтении:* – выделять необходимые факты /сведения; – отделять основную информацию от второстепенной; – определять временную и причинно-следственную взаимосвязь событий и явлений; – обобщать описываемые факты/ явления; – оценивать важность/ новизну/ достоверность информации; – понимать смысл текста и его проблематик, используя элементы анализа текста; – извлекать из текста лексико-грамматические явления с ,целью их распознания и закрепления; • *в письменной речи.* – излагать содержание прочитанного/ прослушанного иноязычного текста в тезисах, рефератах, обзорах; – фиксировать и обобщать письменную информацию, описывать события, факты, явления. – сообщать, запрашивать информацию, выражая собственное мнение, суждение; • *в переводе.* – демонстрировать умение использовать толковые и двуязычные словари и другую справочную литературу для решения переводческих задач; – выполнять полный выборочный письменный перевод: с русского на английский и с английского на русский языки.
	владеть навыками /иметь опыт:	– иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике и навыками устной речи; – навыками реферирования, резюме, биографии на иностранном языке; – навыками публичной речи, ведения дискуссии на иностранном языке.
Содержание:		Курс иностранного языка состоит из 4 основных модулей,

	позволяющих стандартизировать языковой материал и унифицировать требования к развитию тех или иных навыков. Языковая реализация каждого модуля предполагает тематический отбор соответствующих синтаксических структур, лексики, лингвострановедческих и экстралингвистических факторов. Каждый модуль предусматривает комплексное обучение всем видам речевой деятельности, при необходимости с усилением акцента на том или ином из них. Все модули разделены по аспектам языка и видам речевой деятельности. Основными организационными формами обучения являются: аудиторные занятия с преподавателем, текущая внеаудиторная ,работа студентов дома, в лингафонном кабинете, компьютерном классе, по тренировке и самоконтролю усвоения материала, самостоятельная работа студентов под руководством преподавателя как средство усиления индивидуализации. Самостоятельная работа дома предполагает такие виды работы как: подготовка к текущим практическим занятиям; внеаудиторное чтение; перевод научно-технической литературы. Самостоятельная работа в лингафонном кабинете предполагает такие виды работы как: работа с аудио/видео ,материалами; работа с Интернет-ресурсами. Самостоятельная работа имеет такое же методическое и материальное обеспечение, как и аудиторные занятия по иностранному языку. При определении итоговой оценки за курс иностранного языка 30% ее должна составлять оценка самостоятельной работы студентов.
Форма промежуточной аттестации:	Зачет

Название:		Принятие решений и оценка риска в сфере информационной безопасности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-8, ОПК-2, ПК-13
Результаты освоения дисциплины	**знать:**	общую методологию и схему процесса выработки решений; формальные методы и процедуры измерения предпочтений ЛПР для построения функций выбора наилучших альтернатив; технологии оценки эффективности и предпочтительности альтернатив по выбранным критериям в сложных ситуациях.
	уметь:	использовать основные положения теории управления (законы, принципы, методы) в практической работе по управлению техническими системами; использовать современные научные методы анализа проблем и задач, возникающих перед ЛПР в ходе управления; использовать современные методы математической теории принятия решений для решения типовых задач обоснования решений.
	владеть навыками /иметь опыт:	владеть современными научными методами анализа проблем и задач, возникающих перед ЛПР в ходе управления; владеть современными методами математической теории принятия решений для решения типовых задач обоснования решений
Содержание:		Основные задачи принятия решений (ПР) в науке, технике и экономике. Понятие системы. Структура системы. Понятие структуры, основные виды и формы. Понятие иерархических структур. Многоуровневые иерархические системы. Виды и формы представления структур целей. Классификация систем. Основные подходы к классификации систем: абстрактность, искусственность, открытость, целенаправленность и другие категории.

	Автоматизированные системы принятия решений. Экспертные системы. Понятие и структура экспертной системы. Разработка и применение экспертных систем. Инженерия знаний. Основные понятия инженерии знаний. Программные системы поддержки принятий решений. Хранилища данных и OLAP-системы. Интеллектуальный анализ данных (Data Mining).
Форма промежуточной аттестации:	Зачет

Название:		Обеспечение безопасности финансовой и банковской деятельности
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-4, ПК-10, ПСК-1.1
Результаты освоения дисциплины	**знать:**	– методику внедрения Стандарта в кредитно-финансовом учреждении. – подходы к построению системы обеспечения ИБ кредитно-финансового учреждения. – структуру и принципы создания, внедрения и функционирования системы ИБ кредитно-финансового учреждения. – принципы обеспечения ИБ, изложенные в Стандарте. – основные положения Стандарта при разработке нормативно-распорядительных документов обеспечения ИБ кредитно-финансового учреждения. – положения типовых методик оценки рисков нарушения ИБ. – требования Стандарта к модели угроз и нарушителей ИБ кредитно-финансового учреждения. – содержание общих требований политики ИБ. – основные подходы к проектированию системы менеджмента ИБ кредитно-финансовой организации. – требования к эффективному использованию системы мониторинга и аудита процессов обеспечения ИБ
	уметь:	– принимать эффективные решения по интеграции положений и требований Стандарта в систему обеспечения ИБ организации с типовой инфраструктурой. – 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 работы с нормативной документацией по банковской финансовой безопасности, – навыками работы с программно-аппаратными средствами обеспечения информационной безопасности
Содержание:		Место и роль финансовой составляющей в системе обеспечения экономической безопасности банковской деятельности. Экономическое содержание и особенности обеспечения безопасности банковской деятельности. Сущность финансовой безопасности как подсистемы экономической безопасности банковской деятельности. Оценка возможностей предотвращения угроз финансовой безопасности в банковской системе. Факторы обеспечения финансовой составляющей безопасности банковской деятельности. Финансовые регуляторы безопасности и функционирования

	банковской системы. Оценка контрольной среды банка с точки зрения обеспечения его финансовой безопасности. Защитные функции технологий финансового менеджмента в банковской системе. Защита и гарантии возвратности депозитов коммерческих банков. Обеспечение финансовой безопасности коммерческого банка как необходимое условие эффективности банковской деятельности. Обеспечение прибыльности банковской деятельности как показателя ее финансовой безопасности. Роль ликвидности в обеспечении безопасности банковской деятельности. Анализ кредитного портфеля коммерческого банка как основа обеспечения возвратности банковских ресурсов. Особенности формирования региональных систем гарантирования средств клиентов коммерческих банков России. Угрозы безопасности информационных систем. Типы атак на протоколы информационного взаимодействия. Службы защиты. Криптографические методы защиты. Криптосистемы с секретным ключом. Криптосистемы с открытым ключом. Криптографические протоколы. Контроль целостности информации. Методы аутентификации информации. Электронная подпись. Управление ключами. Стандарт X.509. Вероятностное шифрование. Причины ненадежности криптосистем.
Форма промежуточной аттестации:	экзамен

Название:		Проектирование защищенных баз данных
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-7, ПК-13, ПСК-1.1
Результаты освоения дисциплины (модуля)	**знать:**	– основы построения защищённых баз данных; – концепцию защиты информации в проектируемых базах данных; – основные принципы и методы защиты информации в процессе проектирования баз данных; – основные руководящие и нормативные документы по защите информации в проектируемых базах данных; – порядок организации защиты информации в процессе проектируемых базах данных
	уметь:	– выявлять угрозы каналы утечки информации в процессе проектирования баз данных; – описывать (моделировать) объекты защиты и угрозы безопасности информации в проектировании баз данных; – применять наиболее эффективные методы и средства защиты информации в процессе проектирование баз данных; – контролировать эффективность мер защиты
	владеть навыками /иметь опыт:	– Выявления угроз безопасности информации в базах данных; – Обеспечения оптимального уровня защиты информации в проектируемых базах данных
Содержание:		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. 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. Основы реляционной алгебры. Реляционные исчисления, построенные на доменах и кортежах. СУБД Access. Запросы. в СУБД Access и Oracle на основе языка QBEи SQL Организация поиска, фильтрации, сортировки средствами СУБД Access. Этапы и принципы проектирования баз данных. Формирование требований пользователей информационной системы во время проектирования. Повышение производительности запросов в БД. Планы выполнения запросов. Многопользовательский доступ. Транзакция. Управление транзакциями в СУБД Oracle, MS SQL. 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.
Форма промежуточной аттестации:	зачет

Название:		Технические средства охраны
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-12, ПК-14, ПК-15, ПСК-1.4
Результаты освоения дисциплины	**знать:**	– Возможности технических средств охраны; – Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – Основы физической защиты объектов информатизации.
	уметь:	– Пользоваться нормативными документами по физической защите объекта информатизации – Анализировать и оценивать угрозы информационной безопасности объекта;
	владеть навыками /иметь опыт:	– Методами и средствами технической защиты информации; – Проектирования и наладки системы технической защиты.
Содержание:		Основы физической защиты объектов информатизации. Внешние датчики охранной сигнализации. Внутренние датчики охранной сигнализации. Телевизионная система оценки сигнала тревоги. Классификация камер. Организация физической защиты объектов информатизации.
Форма промежуточной аттестации:		Зачет с оценкой

Название:		Комплексное обеспечение защиты информации объекта информатизации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-4, ПК-11, ПК-12, ПСК-1.4
Результаты освоения дисциплины	**знать:**	– место и роль информационной безопасности в системе национальной безопасности Российской Федерации; – современные средства разработки и анализа программного обеспечения на языках высокого уровня; – аппаратные средства вычислительной техники; – операционные системы персональных ЭВМ; – основы администрирования вычислительных сетей; – системы управления базами данных; – 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; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. – анализировать и оценивать угрозы информационной безопасности объекта;
	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; профессиональной терминологией
Содержание:		Изучение подхода к задаче проверки корректности поведения информационных систем – метод верификации моделей программ (model checking). Рассматриваются и обосновываются основные приемы построения моделей информационных систем, включая последовательные и распределенные программы, микроэлектронные схемы, и др., логические средства спецификации их поведения, а также алгоритмы проверки выполнимости спецификаций на заданных моделях программ. Изучаются инструментальные средства верификации моделей для темпоральных логик SMV (Symbolic Model Verifier) и SPIN и их применение для верификации моделей программ и логических схем. При чтении лекций используются компьютерные презентации.
Форма промежуточной аттестации:		экзамен

Название:		Анализ безопасности протоколов
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-10, ПК-15, ПСК-1.4
Результаты освоения дисциплины	**знать:**	– методы анализа и тестирования протоколов; – способы защиты систем; – современные средства отладки и эмуляции программного кода.
	уметь:	– формализовать задачи анализа безопасности; – создавать формальное описание протоколов с целью дальнейшего анализа; – анализировать структуру и состав подсистем безопасности;
	владеть навыками /иметь опыт:	– методами и инструментальными средствами анализа безопасности программного обеспечения, методами и средствами поиска уязвимостей, анализа и верификации протоколов; – практикой получения и анализа аудита событий информационной безопасности.
Содержание:		• Общие сведения о криптографических протоколах. • Понятие атаки на криптографический протокол. • Идентификация и аутентификация. Основные понятия и концепции • Протоколы обмена ключами. • Развитые протоколы обмена ключами с аутентификацией сторон. • Типичные атаки на протоколы аутентификации • • Параметры защиты IP-Sec. • Протоколы защиты данных в сети Internet. • Отказ в аутентификации в основном режиме первой фазы протокола IKE, основанного на цифровой подписи. • Протокол удаленной регистрации SSH. • Депонирование ключей и возможность контроля информационного взаимодействия • Инфраструктура открытых ключей. • Схемы обязательств. • Доказательства с нулевым разглашением. • Системы электронного голосования. • Протокол голосования с несколькими счетными комиссиями. Схемы разделения секрета
Форма промежуточной аттестации:		зачет

Название:	Безопасность систем баз данных
Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:	ПК-2, ПК-4, ПСК-1.2

Результаты освоения дисциплины	**знать:**	– принципы построения и функционирования, примеры реализаций современных систем управления базами данных; – архитектуру систем баз данных; – основные модели данных; – физическую организацию баз данных; – средства обеспечения безопасности данных; – последовательность и содержание этапов проектирования баз данных;
	уметь:	– разрабатывать и администрировать базы данных; – реализовывать политику безопасности баз данных; – выделять сущности и связи предметной области; – отображать предметную область на конкретную модель данных; – нормализовывать отношения при проектировании реляционной базы данных; – создавать объекты базы данных; – выполнять запросы к базе данных; – разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; – применять средства обеспечения безопасности данных;
	владеть навыками /иметь опыт:	– навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; – навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.
Содержание:		Дисциплина "Безопасность систем баз данных" относится к числу дисциплин базовой части профессионального цикла. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями и умениями, сформированными в процессе изучения дисциплин: Дисциплина "Безопасность систем баз данных" является предшествующей для изучения дисциплин "Разработка и эксплуатация защищенных автоматизированных систем" и "Программно-аппаратные средства обеспечения информационной безопасности", а также дисциплин вариативной части профессионального цикла, предусмотренных учебным планом.
Форма промежуточной аттестации:		Зачет, экзамен

Название:		Безопасность сетей ЭВМ
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-6, ПК-10, ПСК1.4
Результаты освоения дисциплины	**знать:**	Понятия, определения ЛВС и ГВС, и их характеристики. Способы и методы обеспечения безопасности ЛВС и ГВС;
	уметь:	Настроить программный маршрутизатор, работать с устройствами, программными продуктами, обеспечивающими безопасность ЛВС и ГВС.
	владеть навыками /иметь опыт:	Навыком проектирования ЛВС и ГВС.
Содержание:		Сетевая архитектура. Функционирование сети. Работа сети, модель

	OSI, многоуровневая архитектура. Взаимодействие уровней модели OSI. Модель IEEE Project 802, расширение модели OSI. Назначение драйверов. Сетевая среда, драйверы и модель OSI. Драйверы и сетевое программное обеспечение, драйвер платы сетевого адаптера. Функции пакетов данных. Структура пакета, основные компоненты. Формирование пакетов, адресация пакета, рассылка пакетов. Назначение протоколов. Работа протоколов, компьютер-отправитель, компьютер-получатель. Маршрутизируемые и немаршрутизируемые протоколы. Стандартные стеки. Стандартные протоколы.
Форма промежуточной аттестации:	Экзамен

	Название:	Безопасность операционных систем
	Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины:	ПК-1, ПК-2, ПСК-1.1
Результаты освоения дисциплины	**знать:**	– основные информационные технологии, используемые в автоматизированных системах; – возможности, классификацию и область применения макрообработки; – показатели качества программного обеспечения; – принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств Unix и Windows;
	уметь:	– проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем;
	владеть навыками /иметь опыт:	– профессиональной терминологией в области информационной безопасности; – навыками проектирования программного обеспечения с использованием средств автоматизации; – навыками работы с современными операционными системами, восстановления операционных систем после сбоев; – навыками установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности; – навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

Содержание:	Определение операционной системы (ОС). Место ОС в программном обеспечении компьютеров, компьютерных систем и сетей. Поколения операционных систем. Назначение, состав и функции ОС. Понятие компьютерных ресурсов. Концепция многоуровневого виртуального компьютера. Операционные оболочки и среды. Архитектуры операционных систем. Классификация ОС. Интерфейсы операционных систем. Эволюция ОС. Эффективность ОС. Однопрограммные, многопрограммные, многопользовательские и многопроцессорные операционные системы. Примеры ОС: MS DOS, Windows 3.x, Windows 9.x/Me/2000/XP/2003/Vista/7, UNIX, Linux, OS/2, Macintosh, MVS, MV. Прикладные операционные среды. Совместимость операционных систем. Виды совместимости. Языковая и двоичная совместимость. Эмуляция. Виртуальные машины и операционные среды. Загрузка операционных систем (на примере Windows XP/2000/2003). Этапы процесса загрузки. Работа загрузчика. Опции загрузочного меню. Выбор аппаратного профиля. Загрузка и инициализация ядра. Загрузка драйверов и сервисов. Регистрация пользователя. Инсталляция и конфигурирование операционных систем. Инсталляция и конфигурирование однопрограммной ОС с текстовым интерфейсом (на примере MS DOS). Подготовка файлов config.sys и autoexec.bat. Программа Setup, алгоритм загрузки ОС. Инсталляция и конфигурирование многопрограммной многопользовательской ОС с графическим интерфейсом (на примере Windows XP/2000/2003). Требования к аппаратным ресурсам. Подготовка процесса инсталляции. Конфигурирование разделов на жестком диске. Выбор файловой системы. Выбор варианта установки (локальная, сетевая). Инсталляция мультиоперационных систем.
Форма промежуточной аттестации:	Зачет, экзамен

Название:		Разработка и эксплуатация защищенных автоматизированных систем
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-2, ПК-15, ПСК-1.1
Результаты освоения дисциплины	**знать:**	– о методах анализа угроз информационной безопасности на этапе построения АС; – о принципах обеспечения информационной безопасности на этапе построения АС; – о технологии обеспечения защиты на этапе создания АС; – о типичных атаках на АС в процессе ее создания; – методологические и технологические основы обеспечения безопасности информации при создании АС; – виды, источники и носители защищаемой информации на этапе построения АС; – основные угрозы безопасности информации при построении АС; – концепцию защиты информации при построении АС; – основные принципы и методы защиты информации на этапе построения АС; – основные руководящие и нормативные документы по защите информации на этапе создания АС;

		– порядок организации защиты информации при построении АС.
	уметь:	– выявлять угрозы и каналы утечки информации при создании АС; – описывать (моделировать) объекты защиты и угрозы безопасности информации на этапе проектирования АС; – применять наиболее эффективные методы и средства защиты информации при создании АС; – контролировать эффективность мер защиты;
	владеть навыками /иметь опыт:	– использования критериев оценки защищенности в создаваемой АС; – использования критериев оценки защищенности создаваемых АС; – работы с документацией, используемой при построении АС.
Содержание:		Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем. Понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы. Методы проектирования сложных систем. Уровни проектирования. Структуризация предметной области, построение ее инфологической модели. Основные этапы проектирования, их особенности. Основные объекты проектирования: их классификация и характеристики. Структурный подход к проектированию сложных систем (CMO, DFD, SADT). Методология построения автоматизированных систем. Стадии разработки автоматизированных систем. Предпроектный анализ, концептуальное, логическое и физическое проектирование. Принципы автоматизированного проектирования. Особенности макро и микропроектирования. Виды обеспечений этапа микропроектирования. Архитектура защищенных систем. Принципы построения защищенных информационных систем. Реализация систем контроля доступа. Практические методы реализации моделей безопасности. Способы представления информации о правах доступа. Ядро безопасности и мониторинг взаимодействий в системе. Технологический цикл реализации защищённой системы обработки и хранения информации. Общее содержание основных работ по защите информации. Организация работ по защите. Функции и правовые отношения заказчиков и разработчиков. Система типовых документов по защите информации. Методы построения обобщенных критериев. Экспертные методы оценок критериев. Анализ характеристик системы управления на основе информационного графа. Вычисление структурно – топологических характеристик систем управления. Вычисление числовых характеристик системы управления с помощью задания числовой функции на структурном графе системы. Способы описания структурного сопряжения элементов. Распределение задач управления по узлам. Разработка политики безопасности. Настройка прав доступа к объектам БД в СУБД. Настойка регистрации системны событий средствами СУБД. Программная реализация механизма регистрации доступа к полям и строкам таблицы. Разработка подсистемы идентификации и установление подлинности пользователя и программного продукта. Разработка подсистемы конфиденциальности данных и сообщений. Разработка подсистемы целостности данных и сообщений.
Форма промежуточной аттестации:		Экзамен

Название:		Элективные дисциплины по физической культуре и спорту
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ОК-9
Результаты освоения дисциплины	**знать:**	влияние оздоровительных систем физического воспитания на укрепление здоровья, профилактику профессиональных заболеваний и вредных привычек; способы контроля и оценки физического развития и физической подготовленности; правила и способы планирования индивидуальных занятий различной целевой направленности
	уметь:	выполнять индивидуально подобные комплексы оздоровительной и адаптивной (лечебной) физической культуры, композиции ритмической и аэробной гимнастики, комплексы упражнения атлетической гимнастики; выполнять простейшие приемы самомассажа и релаксации; преодолевать искусственные и естественные препятствия с использованием разнообразных способов передвижения; выполнять приемы защиты и самообороны, страховки и самостраховки; осуществлять творческое сотрудничество в коллективных формах занятий физической культурой
	владеть навыками /иметь опыт:	средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры личности для успешной социально-культурной и профессиональной деятельности
Содержание:		
Форма промежуточной аттестации:		Зачет

Название:		Алгоритмы направленного перебора
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-2, ПСК-1.3
Результаты освоения дисциплины (модуля)	**знать:**	– методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; – современные средства разработки и анализа программного обеспечения на языках высокого уровня; – принципы построения информационных систем.
	уметь:	– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные.
	владеть навыками /иметь опыт:	– методами анализа и формализации информационных процессов объекта и связей между ними; – профессиональной терминологией.

Содержание:	Определения алгоритма. История. Оценка сложности алгоритмов. Переборные задачи на графах. Реализация полного перебора. Комбинаторные задачи. Поиск в дереве и на графах. Методы сокращенного перебора и эвристики. Методы ветвей и границ. Метод альфа бета отсечений. Генетические алгоритмы. Арифметика больших чисел. Эффективные алгоритмы. Разложение больших чисел на простые множители. Распределенные вычисления. Распределенные вычислительные системы и их применение. Нейронная сеть. Методы криптоанализа. Дифференциальный метод. Методы криптоанализа. Линейный метод. Методы криптоанализа. Решеточный метод. Задача о ферзях. Решение ребусных задач методом перебора. Распределенная система подбор пороля. Методы ветвей и границ. Генетические алгоритмы. Разложение больших чисел на простые множители. Разложение больших чисел на простые множители Линейный метод. Решеточный метод.
Форма промежуточной аттестации:	Зачет

Название:		Комбинаторные алгоритмы
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-2, ПСК-1.3
Результаты освоения дисциплины (модуля)	**знать:**	– методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; – современные средства разработки и анализа программного обеспечения на языках высокого уровня; – принципы построения информационных систем.
	уметь:	– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные.
	владеть навыками /иметь опыт:	– методами анализа и формализации информационных процессов объекта и связей между ними; – профессиональной терминологией.
Содержание:		Определения алгоритма. История. Оценка сложности алгоритмов. Переборные задачи на графах. Реализация полного перебора. Комбинаторные задачи. Поиск в дереве и на графах. Методы сокращенного перебора и эвристики. Методы ветвей и границ. Метод альфа бета отсечений. Генетические алгоритмы. Арифметика больших чисел. Эффективные алгоритмы. Разложение больших чисел на простые множители. Распределенные вычисления. Распределенные вычислительные системы и их применение. Нейронная сеть. Методы криптоанализа. Дифференциальный метод. Методы криптоанализа. Линейный метод. Методы криптоанализа. Решеточный метод. Задача о ферзях. Решение ребусных задач методом перебора. Распределенная система подбор пороля. Методы ветвей и границ. Генетические алгоритмы. Разложение больших чисел на простые множители. Разложение больших чисел на простые множители Линейный метод. Решеточный метод.
Форма промежуточной		Зачет

аттестации:	

Название:		**Безопасность в Интернет/Интранет**
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-2, ПК-13, ПСК-1.1
Результаты освоения дисциплины (модуля)	**знать:**	основные руководящие и нормативные документы по защите информации в INTERNET/INTRANET; виды, источники и носители защищаемой информации в INTERNET/INTRANET; основные угрозы безопасности информации в INTERNET; концепцию защиты информации в INTERNET/INTRANET; основные принципы и методы защиты информации в INTERNET/INTRANET; порядок организации защиты информации в INTERNET/INTRANET.
	уметь:	обосновывать практическую и теоретическую ценность полученных результатов; консультироваться, проверять факты, анализировать ситуации с различных точек зрения выявлять угрозы и каналы утечки информации в INTERNET/INTRANET; описывать (моделировать) объекты защиты и угрозы безопасности информации в INTERNET/INTRANET; применять наиболее эффективные методы и средства защиты информации в INTERNET/INTRANET; контролировать эффективность мер защиты.
	владеть навыками /иметь опыт:	Навыками сбора, обработки, анализа и систематизации научно-технической информации по обеспечению безопасности в Интернет/Интранет, выбор методик и средств решения задачи работы в сети INTERNET; Навыками программирования в сети INTERNET; Владеть навыками выявления угроз безопасности в сети INTERNET/INTRANET; Навыками обеспечения оптимального уровня защиты в сети.
Содержание:		Организационная структура Интернет. Угрозы безопасности. Организационная структура Интернет. Эталонная модель TCP/IP. Состав и назначение сетевых протоколов. Основные сетевые приложения и сервисы сети Интернет. Угрозы информационной безопасности для систем обработки информации, использующих Интернет. Cookies. Уязвимые места и причины их возникновения Обзор подходов к обеспечению информационной безопасности. Схема адресации в сети Интернет. Числовые IP-адреса. Адресация сетей и подсетей. Классы адресов, использование пар адрес/маска. TCP-адреса и UDP-адреса. Адресация сервисов. Символические адреса. Система доменных имен. DNS-серверы. Протоколы передачи данных. Назначение и функциональные возможности. Протоколы IP, ICMP, UDP. Их назначение, формат пакетов и дейтаграмм. Протокол TCP: назначение и основные функциональные возможности, формат сообщений, обеспечение гарантированной передачи данных, установление и разрыв соединения.

	Протоколы защищенной передачи данных. Назначение протоколов SSL, SSH, PGP, IPSec, PPTP, L2TP. Протокол HTTP. Назначение и представляемые услуги. Формат сообщений. Анализ полей заголовка сообщения. Методы (запросы) и коды возврата. Установление и разрыв соединения, пролонгированное соединение. Функции сервера, клиента, промежуточного сервера. Кэширование информационных ресурсов. Взаимодействие с сервером proxy. Метаязык SGML – средство порождения языков разметки. Отношение между языками SGML, HTML, XML. Расширяемость XML. Описание языка XML. Обзор приложений XML Преимущества и ограничения данного подхода Язык разметки HTML. Назначение. Основные концепции. Тэги форматирования. Включение иллюстраций. Гипертекстовые ссылки. Структурирование документа и поддержка диалога с пользователем. Раздел 3. Обеспечение безопасности в Интернет/Интранет. Действие в случае взлома защиты INTERNET. Контроль за работой пользователей в INTERNET. Использование программных средств в INTERNET. Администратор безопасности в INTERNET Нападение с использованием сетевых протоколов: «летучая смерть», SYN- бомбардировка, спуффинг на основе протокола ICMP ARP-spoofing или ложный ARP- сервер, IP-Hijacking, другие примеры атак. Сетевые вирусы в INTERNET. Атаки, основные на ошибках при программировании и на слабостях технологий JAVA иActive. Слабости системных утилит, команд и служб INTERNET. Shell как средство замены уязвимых сервисов TCP/ IP. Межсетевые экраны (МЭ): типы МЭ, виртуальные сети, схема подключения МЭ, основные компоненты МЭ, сертифицированные МЭ. Шифрование в INTERNET: аппаратное и программное шифрование, протоколы со встроенными возможностями шифрования, криптокарта Fortezza, сканеры. Средства мониторинга сетевой безопасности. Аутентификация в INTERNET. Улучшение паролей. Серверы аутентификации. Основные технологии доступа к базам данных при помощи INTERNET. Доступ на стороне клиента и на стороне сервера. Коннектор баз данных IDC. Сценарий и шаблоны IDC. Семейство продуктов PALINDROME. Сетевое резервное копирование. Зеркальные серверы. Удалённые атаки на INTERNET и задачи её защиты. Классические методы взлома корпоративных сетей: подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия
Форма промежуточной аттестации:	зачет

Название:		Защита абонентского телетрафика
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-2, ПК-13, ПСК-1.1
Результаты освоения дисциплины	**знать:**	– виды, источники и носители защищаемой информации; – основные угрозы безопасности информации; – концепцию инженерно-технической защиты информации; – основные принципы и методы защиты информации; – основные руководящие и нормативные документы по инженерно-технической защите информации;

		– порядок организации инженерно-технической защиты информации;
	уметь:	– выявлять угрозы и технические каналы утечки информации; – описывать объекты защиты и угрозы безопасности информации; – применять наиболее эффективные методы и средства инженерно-технической защиты информации; – контролировать эффективность мер защиты
	владеть навыками /иметь опыт:	– навыками аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем, инженерного расчета размеров контролируемой зоны
Содержание:		Введение. Этапы развития радиотелефонной связи с подвижными объектами. Предпосылки разработки стандарта GSM. Организация радиоканалов. Проблемы, возникающие при организации радиоканалов и методы их устранения. Исходные данные, особенности и этапы планирования сотовой сети. Кодирование речевой информации и линейное кодирование в GSM. Понятия дифференциальной импульсно-кодовой модуляции и вокодеров. Необходимость и особенности линейного кодирования в GSM. Идеология построения GSM. Система нумерации. Функциональное построение GSM и назначение функциональных блоков. Особенности процесса обслуживания вызовов в сотовых сетях. Подключение, отключение, блуждание, переключение вызова, обновление данных местонахождения, поиск и т.д. Организация физических и логических каналов в GSM. Организация физических каналов. Понятие - кодовая комбинация, форматы; кодовых комбинаций и их формирование. Пользовательские логические каналы и логические каналы управления. Разновидности логических каналов управления и их назначение. Организация логических каналов. Системны сигнализации, используемые в GSM. Сигнализация в процессе обслуживания вызова
Форма промежуточной аттестации:		Зачет

Название:		Нормативно-распорядительная документация в сфере обеспечения безопасности государства
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-8, ПК-9, ПСК-1.1
Результаты освоения дисциплины	**знать:**	место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты

		государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
	уметь:	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;
	владеть навыками /иметь опыт:	навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности;
Содержание:		Правовой аспект проблемы общей теории безопасности России. 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 российской федерации. Основные источники угроз национальной безопасности России. 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:		Зачет

Название:		Законодательство в области телекоммуникаций
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-8, ПК-9, ПСК-1.1
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 России.

	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 российской федерации. Основные источники угроз национальной безопасности России. 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:	зачет

Название:		Основы алгоритмизации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-2, ПСК-1.3
Результаты освоения дисциплины	**знать:**	базовые понятия теории алгоритмов; технологию разработки профессиональных программ (алгоритмизацию); один – два рабочих языка объектно-ориентированного программирования; основные виды программного обеспечения современных ЭВМ для объектно-ориентированного программирования; методику объектно-ориентированного анализа и проектирования.
	уметь:	пользоваться современными аппаратными средствами; согласованно решать задачи разработки эффективных моделей данных и алгоритмов их обработки при создании прикладного программного обеспечения, а также получать программные реализации на языках высокого уровня; Работать с инструментальной системой программирования Microsoft Visual Studio .NET;
	владеть навыками /иметь опыт:	навыками разработки алгоритмов и программ решения прикладных задач на языке высокого уровня в среде объектно-ориентированного программирования.
Содержание:		Порядок решения инженерной задачи с помощью ЭВМ. Математическая модель. Методы решения задач. Спецификация алгоритма. Структуры алгоритмов. Способы описания алгоритмов. Структурный подход к разработке алгоритмов. Алгоритмы численных методов. Алгоритмизация простейших задач. Языки программирования, их свойства. Основы алгоритмизации и программирования задач на языке высокого уровня. Понятие файла; Статические и динамические данные; сложные структуры данных (списки, деревья, сети); потоки ввода-вывода; Основные принципы и подходы проектирования структурированных алгоритмов. Методы и средства объектно-ориентированного программирования; Рекурсия и итерация; сортировка и поиск. Стандарты на разработку прикладных программных средств. Документирование, сопровождение и эксплуатация программных средств.
Форма промежуточной аттестации:		Зачет с оценкой

Название:		Алгоритмы и структуры данных
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-2, ПСК-1.3
Результаты освоения дисциплины	**знать:**	базовые понятия теории алгоритмов; технологию разработки профессиональных программ (алгоритмизацию); один – два рабочих языка объектно-ориентированного программирования; основные виды программного обеспечения современных ЭВМ для объектно-ориентированного программирования; методику объектно-ориентированного анализа и проектирования.
	уметь:	пользоваться современными аппаратными средствами; согласованно решать задачи разработки эффективных моделей данных и алгоритмов их обработки при создании прикладного программного обеспечения, а также получать программные реализации на языках высокого уровня; Работать с инструментальной системой программирования Microsoft Visual Studio .NET;
	владеть навыками /иметь опыт:	навыками разработки алгоритмов и программ решения прикладных задач на языке высокого уровня в среде объектно-ориентированного программирования.
Содержание:		Порядок решения инженерной задачи с помощью ЭВМ. Математическая модель. Методы решения задач. Спецификация алгоритма. Структуры алгоритмов. Способы описания алгоритмов. Структурный подход к разработке алгоритмов. Алгоритмы численных методов. Алгоритмизация простейших задач. Языки программирования, их свойства. Основы алгоритмизации и программирования задач на языке высокого уровня. Понятие файла; Статические и динамические данные; сложные структуры данных (списки, деревья, сети); потоки ввода-вывода; Основные принципы и подходы проектирования структурированных алгоритмов. Методы и средства объектно-ориентированного программирования; Рекурсия и итерация; сортировка и поиск. Стандарты на разработку прикладных программных средств. Документирование, сопровождение и эксплуатация программных средств.
Форма промежуточной аттестации:		зачет

Название:		Криптографические протоколы
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-1, ПК-4, ПК-15, ПСК-1.2
Результаты освоения дисциплины	**знать:**	– формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям; – криптографические стандарты; – типовые криптографические протоколы и основные требования к ним; – принципы построения криптографических хеш-функций; – основные схемы цифровой подписи;

		– протоколы идентификации; – протоколы передачи и распределения ключей;
	уметь:	– использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов; – формулировать свойства безопасности криптографических протоколов; – проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;
	владеть навыками /иметь опыт:	– криптографической терминологией; – простейшими подходами к анализу безопасности криптографических протоколов
Содержание:		Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол Стандарт X.509. Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации. Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. Забывающая передача информации. Протокол подписания контракта. Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязываемости. Протоколы электронных платежей и цифровых денег Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Проблемы автоматизации анализа криптографических протоколов. Итоги изучения дисциплины.
Форма промежуточной аттестации:		Зачет

Название:		Защита сетевых проколов
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-1, ПК-4, ПК-15, ПСК-1.2
Результаты освоения дисциплины	**знать:**	– формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям; – криптографические стандарты; – типовые криптографические протоколы и основные требования к ним; – принципы построения криптографических хеш-функций; – основные схемы цифровой подписи; – протоколы идентификации; – протоколы передачи и распределения ключей;
	уметь:	– использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов; – формулировать свойства безопасности криптографических протоколов; – проводить сравнительный анализ криптографических

		протоколов, решающих сходные задачи;
	владеть навыками /иметь опыт:	– криптографической терминологией; – простейшими подходами к анализу безопасности криптографических протоколов
Содержание:		Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол Использование симметричных и асимметричных шифросистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов. Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля. Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото. Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов. Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Схемы предварительного распределения ключей. Неравенство Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции Блома. Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации. Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. Забывающая передача информации. Протокол подписания контракта.
Форма промежуточной аттестации:		Зачет

Название:	Администрирование информационных систем
Название и номер направления и/или специальности:	10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ПК-3, ПК-5, ПК-13, ПСК-1.2

Результаты освоения дисциплины (модуля)	**знать:**	аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления базами данных; 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:	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. анализировать и оценивать угрозы информационной безопасности объекта;
	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; профессиональной терминологией.
Содержание:		Информационные системы: общие характеристики. Понятие администрирования. Администрирование операционной системы. Общие сведения об операционных системах. Основы администрирования ОС Microsoft Windows. Основы администрирования ОС Linux. Информационные сети и их администрирование. Основы безопасности. IT-бакалавр: навыки общения. Поиск и устранение неполадок
Форма промежуточной аттестации:		Зачет

Название:		Современные цифровые технологии сетей передачи данных
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-3, ПК-5, ПК-13, ПСК-1.2
Результаты освоения дисциплины (модуля)	**знать:**	основные характеристики и возможности используемых и перспективных сетевых технологий; основы администрирования вычислительных сетей; принципы построения и функционирования систем и сетей передачи информации; основные телекоммуникационные протоколы; 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:	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

		осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта.
	владеть навыками /иметь опыт:	методами и средствами выявления угроз безопасности автоматизированным системам; методами анализа и формализации информационных процессов объекта и связей между ними; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; профессиональной терминологией
Содержание:		История создания аналоговых голосовых сетей передачи данных. Недостатки аналоговых сетей передачи данных. Гибридные сети передачи голосовых данных, преимущества. Основные принципы построения VOIP сетей передачи данных. Протоколы VOIP телефонии. Обзор оборудования и программного обеспечения реализующего IP телефонию. Протокол SCCP. Базовые принципы функционирования. Типовые схемы внедрения. Создание VoIP сети с разделением данных и голоса с использованием протокол SCCP. Протокол SIP. Базовые принципы функционирования. Типовые схемы внедрения. Создание VoIP сети с разделением данных и голоса с использованием протокола SIP. Обеспечение защиты голосовой информации в VOIP сетях передачи данных. Перспективы развития VOIP сетей передачи данных.
Форма промежуточной аттестации:		Зачет

Название:		Особенности аттестации объектов информатизации
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-5
Результаты освоения дисциплины	**знать:**	1. нормативные правовые акты; 2. методы организации и обеспечения режима секретности; 3. способы формирования требований по защите информации; 4. проведение контроля мероприятий по защите информации
	уметь:	1. применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности и ее контроля; 2. разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по аттестации;
	владеть навыками /иметь опыт:	1. организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; 2. организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; 3. организации работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации

		средств защиты информации.
Содержание:		Объект информатизации. Требования защищенности АС. Руководящие документы. Требования защищенности защищаемых помещений Исходные данные по аттестуемым объектам информатизации. Программа проведения аттестационных испытаний объектов информатизации. Каналы утечки информации. Основные термины и определения. Содержание и порядок проведения аттестационных испытаний автоматизированных систем Технические каналы утечки речевой информации. И способы их блокировки. Составление технического паспорта и модели угроз по заданию. Измерение ПЭМИ. Измерение наводок в линиях передачи информации. Проверка разрешительной системы доступа Проверка подсистемы гарантированного уничтожения информации Проверка подсистемы аудита Измерение акустического и виброакустического сигнала Измерение электроакустического сигнала во вспомогательных технических средствах и системах Руководящие документы ФСТЭК. Нормативные документы ФСБ
Форма промежуточной аттестации:		Зачет

Название:		Технологии и средства обнаружения пропаганды экстремизма и терроризма в сети "Интернет"
Название и номер направления и/или специальности:		10.03.01 Информационная безопасность
Компетенции обучающегося, формируемые в результате освоения дисциплины:		ПК-2, ПК-13, ПСК-1.1
Результаты освоения дисциплины	**знать:**	основные руководящие и нормативные документы по защите информации в INTERNET/INTRANET; виды, источники и носители защищаемой информации в INTERNET/INTRANET; основные угрозы безопасности информации в INTERNET; концепцию защиты информации в INTERNET/INTRANET;
	уметь:	обосновывать практическую и теоретическую ценность полученных результатов; консультироваться, проверять факты, анализировать ситуации с различных точек зрения выявлять угрозы и каналы утечки информации в INTERNET/INTRANET; описывать (моделировать) объекты защиты и угрозы безопасности информации в INTERNET/INTRANET; применять наиболее эффективные методы и средства защиты информации в INTERNET/INTRANET; контролировать эффективность мер защиты.
	владеть навыками /иметь опыт:	Навыками сбора, обработки, анализа и систематизации научно-технической информации по обеспечению безопасности в Интернет/Интранет, выбор методик и средств решения задачи работы в сети INTERNET; Навыками программирования в сети INTERNET; Владеть навыками выявления угроз безопасности в сети INTERNET/INTRANET; Навыками обеспечения оптимального уровня защиты в сети.
Содержание:		Организационная структура Интернет. Угрозы безопасности. Основные сетевые приложения и сервисы сети Интернет. Угрозы информационной безопасности для систем обработки информации, использующих Интернет. Cookies. Уязвимые места и

	причины их возникновения Обзор подходов к обеспечению информационной безопасности. Схема адресации в сети Интернет. Числовые IP-адреса. Адресация сетей и подсетей. Классы адресов, использование пар адрес/маска. TCP-адреса и UDP-адреса. Адресация сервисов. Символические адреса. Система доменных имен. DNS-серверы. Протоколы передачи данных. Назначение и функциональные возможности. Протоколы IP, ICMP, UDP. Их назначение, формат пакетов и дейтаграмм. Протокол TCP: назначение и основные функциональные возможности, формат сообщений, обеспечение гарантированной передачи данных, установление и разрыв соединения. Протоколы защищенной передачи данных. Назначение протоколов SSL, SSH, PGP, IPSec, PPTP, L2TP. Протокол HTTP. Назначение и представляемые услуги. Формат сообщений. Анализ полей заголовка сообщения. Методы (запросы) и коды возврата. Установление и разрыв соединения, пролонгированное соединение. Функции сервера, клиента, промежуточного сервера. Кэширование информационных ресурсов. Взаимодействие с сервером proxy. Метаязык SGML – средство порождения языков разметки. Отношение между языками SGML, HTML, XML. Расширяемость XML. Описание языка XML. Обзор приложений XML Преимущества и ограничения данного подхода Язык разметки HTML. Назначение. Основные концепции. Тэги форматирования. Включение иллюстраций. Гипертекстовые ссылки. Структурирование документа и поддержка диалога с пользователем. Раздел 3. Обеспечение безопасности в Интернет/Интранет. Действие в случае взлома защиты INTERNET. Контроль за работой пользователей в INTERNET. Использование программных средств в INTERNET. Администратор безопасности в INTERNET Нападение с использованием сетевых протоколов: «летучая смерть», SYN- бомбардировка, спуффинг на основе протокола ICMP ARP-spoofing или ложный ARP- сервер, IP-Hijacking, другие примеры атак. Сетевые вирусы в INTERNET. Атаки, основные на ошибках при программировании и на слабостях технологий JAVA иActive. Слабости системных утилит, команд и служб INTERNET. Shell как средство замены уязвимых сервисов TCP/ IP. Межсетевые экраны (МЭ): типы МЭ, виртуальные сети, схема подключения МЭ, основные компоненты МЭ, сертифицированные МЭ. Шифрование в INTERNET: аппаратное и программное шифрование, протоколы со встроенными возможностями шифрования, криптокарта Fortezza, сканеры. Средства мониторинга сетевой безопасности. Аутентификация в INTERNET. Улучшение паролей. Серверы аутентификации. Основные технологии доступа к базам данных при помощи INTERNET. Доступ на стороне клиента и на стороне сервера. Коннектор баз данных IDC. Сценарий и шаблоны IDC. Семейство продуктов PALINDROME. Сетевое резервное копирование. Зеркальные серверы. Удалённые атаки на INTERNET и задачи её защиты. Классические методы взлома корпоративных сетей: подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия
Форма промежуточной аттестации:	Зачет