Аннотации рабочих программ дисциплин (модулей) образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Анализ безопасности информационных систем»

Название:		**История**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-3, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	– основные направления, проблемы, теории и методы истории; – основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; – 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:	– анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности; – 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 публичной речи, аргументации, ведения – дискуссии и полемики; – навыками письменного аргументированного изложения – собственной точки зрения; – 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:	**Философия**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-1, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	– содержание и взаимосвязь основных принципов, законов, – понятий и категорий гуманитарных, социальных и – экономических наук; – основные этапы развития философской мысли, основную проблематику и структуру философского знания; – 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:	– использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; – анализировать мировоззренческие, социально и личностно значимые философские проблемы; – 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:	- основными методами научного познания; – 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:		**Иностранный язык**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-7,ОК-8, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	– лексический и грамматический минимум в объеме, – необходимом для работы с текстами профессиональной – направленности и осуществления коммуникации на иностранном языке; – 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:	– читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; – 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 получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке; – 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:	**Правоведение**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-4, ОПК-6
Результаты освоения дисциплины (модуля)	**знать:**	– основы права и законодательства России, основы конституционного строя 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 основные правовые акты, давать правовую оценку информации, – используемой в профессиональной деятельности; – 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 экономических знаний**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-2, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	– основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов; – основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной, деятельности (применительно к отрасли обеспечения информационной безопасности); – 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:	– анализировать экономические показатели деятельности подразделения; – - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; – 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. Экономические потребности и блага; экономические ресурсы и их классификация; экономические субъекты и экономические рынки; кругооборот расходов и доходов; экономическая эффективность; кривая производственных возможностей; краткосрочный и долгосрочный периоды в экономическом анализе; экономический рост и пути его достижения; методы экономической теории и уровни экономического анализа, экономическая стратегия и экономическая политика; экономические ограничения; неопределенность и экономические риски, конкуренция и ее виды; страхование, экономическая безопасность; понятие и виды собственности. Микроэкономика. Теория потребительского поведения; закон убывающей предельной полезности; эффект замещения и эффект дохода; функции спроса и предложения; рыночное равновесие; государственное регулирование рынка; эластичность спроса и предложения и ее зависимость от фактора времени; основные типы рыночных структур: совершенная конкуренция, монополия, олигополия и монополистическая конкуренция; естественная монополия; ценовая дискриминация; кривые спроса и предложения для предприятий, работающих в различных моделях рынка; экономические последствия монополии для общества; антимонопольное законодательство; тайный сговор олигополистов и его последствия; ресурсы предприятия и эффективность их использования; производственная функция и ее

	свойства; закон убывающей предельной производительности; понятие валового, среднего и предельного продукта, выручки и издержек; оптимизация издержек; переменные и постоянные издержки; бухгалтерские и экономические издержки и прибыль; максимизация прибыли в различных моделях рынка; особенности рынка факторов производства; максимизация прибыли и минимизация затрат на рынке ресурсов; рынок труда и заработная плата; оптимизация объема используемых трудовых ресурсов; влияние государства и профсоюзов на рынок труда; особенности рынка физического капитала; потоки и запасы; чистая приведенная стоимость; внутренняя норма доходности; спрос и предложение на земельные ресурсы; экономическая рента; общее равновесие и благосостояние; неравенство в распределении доходов; роль государства. Понятие предприятия, классификация; внешняя и внутренняя среда; диверсификация, концентрация и централизация производства; открытие и закрытие предприятий, санация и банкротство; инфраструктура бизнеса. Макроэкономика. Общественное воспроизводство; макроэкономические субъекты и макроэкономические рынки; основное макроэкономическое тождество; экономические функции правительства; основные макроэкономические показатели; методы измерения валового внутреннего продукта; совокупный спрос и совокупное предложение; макроэкономическое равновесие; безработица и ее виды; инфляция и ее причины; теории экономического роста и экономического цикла; понятие и функции налогов; бюджетно-налоговая политика; денежное обращение; банковская система и ее уровни; банковский и денежный мультипликатор; денежно-кредитная политика; международные экономические отношения; платежный баланс страны; валютный курс; государственный бюджет; закрытая и открытая экономика; теневая экономика; стабилизационная политика. 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:		**Информатика**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	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:	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:	навигацией по файловой структуре компьютера и управления файлами; технологией создания научно-технической документации различной сложности с помощью текстового редактора; технологией решения типовых информационных и вычислительных задач с помощью табличного процессора; технологией решения типовых математических задач с помощью математических пакетов; 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. Защита от несанкционированного вмешательства в информационные процессы. Вычислительная техника. Компьютер. Классификация персональных компьютеров. Состав вычислительной системы (вычислительного комплекса). Аппаратное и программное обеспечение. Классификация служебных и прикладных программных средств. Устройство персонального компьютера. Базовая аппаратная конфигурация. Операционные системы персональных компьютеров. Понятие и назначение операционных систем. Функции и режимы работы операционных систем. Виды операционных систем. Организация файловой системы. Графические редакторы. Текстовый редактор. Форматирование. Хранение и печать документов. Шаблоны документов. Мастер формул. Электронные таблицы. Базы данных. Основные функции баз данных. Сортировка и фильтрация записей. Алгоритмизация и программирование. Этапы решения задач на ПЭВМ. Понятие алгоритма. Свойства и способы описания алгоритмов. Графический способ описания. Основные графические символы. Базовые конструкции алгоритмов (линейная, циклическая, разветвленная). Понятие цикла. Виды циклов. Программирование. Алгоритмические языки. Объектно-ориентированное программирование. Локальные и глобальные сети ЭВМ. Основные понятия в вычислительных сетях. Локальные сети. Топология. Особенности построения и управления вычислительных сетей. Глобальная сеть Internet. Общая характеристика, особенности построения.
Форма промежуточной аттестации:		Экзамен

Название:		**Физика**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуль):		ОК-8, ОПК-1
Результаты освоения дисциплины	**знать:**	основные законы физики;
	уметь:	строить математические модели физических явлений, проводить физический эксперимент, анализировать результаты эксперимента;

	владеть навыками /иметь опыт:	основными методами теоретического и экспериментального исследования физических явлений.
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:		**Безопасность жизнедеятельности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-7
Результаты освоения дисциплины (модуля)	**знать:**	Предельные значения вредных и опасных производственных факторов, поражающих человека, и порядок оказания первой доврачебной помощи при возможных последствиях аварий, катастроф, стихийных бедствий
	уметь:	Различать степени поражения человека опасными факторами в условиях аварий, катастроф, стихийных бедствий и пользоваться средствами индивидуальной защиты, аптечками первой помощи и медицинскими пакетами.
	владеть навыками /иметь опыт:	Определения вредных и опасных производственных факторов в условиях аварий, катастроф, стихийных бедствий; применения и использования средств индивидуальной и коллективной защиты; оказания первой доврачебной медицинской помощи
Содержание:		Организационные и правовые основы безопасности жизнедеятельности Классификация риска и опасностей. Организация безопасных условий труда на предприятиях. Оценка качества производственной среды. Эргономическое обеспечение систем и средств связи. Оценка качества производственной среды. Анализ условий труда: производственный травматизм и профессиональные заболевания; расследование и учет производственного травматизма и методы анализа травматизма. Санитарно-гигиенические факторы производственной среды. Основы электробезопасности. Расчет заземления. Безопасность в чрезвычайных ситуациях на предприятиях связи . Психология поведения человека в условиях ЧС. Устойчивость работы объектов экономики в условиях ЧС мирного и военного времени. Безопасность и экологичность систем и средств связи. Оказание первой доврачебной медицинской помощи в условиях ЧС при поражении вредными и опасными производственными факторами. Организация защиты населения в мирное и военное время, организация ГО в образовательных учреждениях, борьба с терроризмом. Расчет путей эвакуации. Средства индивидуальной защиты и защитные сооружения ГО. Особенности применения СИЗ.

Форма промежуточной аттестации:	Зачет

	Название:	**Физическая культура и спорт**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-9
Результаты освоения дисциплины (модуля)	**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, зачет

Название:		**Теория информации**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-5, ОПК-5
Результаты освоения дисциплины (модуля)	**знать:**	основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; - основные результаты о кодировании при наличии и отсутствии шума; - основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи;
	уметь:	строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; - определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; вычислять теоретико-информационные характеристики источников сообщений и каналов связи; - решать типовые задачи кодирования и декодирования; 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;
	владеть навыками /иметь опыт:	- основами построения математических моделей систем передачи информации; - навыками применения математического аппарата для решения прикладных теоретико-информационных задач; - навыками пользования библиотеками прикладных программ для решения прикладных математических задач; - 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).
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 (источники информации; энтропия источников; дискретный источник без памяти; теоремы Шеннона об источниках; марковские и эргодические источники; информационная дивергенция). 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 Коды Боуза-Чоудхури-Хоквингема. БЧХ-коды. Достоинства и недостатки. Циклические коды, исправляющие две ошибки. Циклические коды, исправляющие пакет ошибок. 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:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-8, ОПК-2
Результаты освоения дисциплины (модуля)	**знать:**	основные понятия и методы линейной алгебры и теории алгебраических систем; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основные задачи аналитической геометрии основные понятия и методы линейной алгебры и теории алгебраических систем; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основные задачи аналитической геометрии
	уметь:	решать основные задачи векторной алгебры и аналитической геометрии; 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; использовать программные и аппаратные средства персонального компьютера; использовать математические методы и модели для решения прикладных зада;
	владеть навыками /иметь опыт:	реализации методов аналитической геометрии и векторной алгебры; линейной алгебры; методов количественного анализа процессов обработки, поиска и передачи информации
	Содержание:	− Целые числа и основы теории делимости. − Основы теории сравнений. − Основные алгебраические структуры. − Кольца матриц. − Системы линейных уравнений. − Кольца многочленов. − Геометрические векторы иих координаты. − Аналитическая геометрияна плоскости. − Аналитическая геометрия в пространстве.

Форма промежуточной аттестации:	Экзамен

	Название:	**Математический анализ**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-8, ОПК-2
Результаты освоения дисциплины (модуля)	**знать:**	– математический анализ (дифференциальное и интегральное исчисление) функции одной и нескольких переменных; – - теорию дифференциальных уравнений и уравнений в частных производных; – - теорию поля.
	уметь:	– Применять методы математического анализа для решения прикладных задач, выбрать соответствующий математический аппарат для решения и контроля правильности решения. –
	владеть навыками /иметь опыт:	– Применения элементами математического анализа для решения профессиональных задач
	Содержание:	– Предел и непрерывность функции. – Дифференциальное исчисление функции одной переменной. – Неопределенный интеграл. – Определенный интеграл. – Дифференциальное исчисление функции многих переменных. – Кратные интегралы. – Теория поля. – Дифференциальные уравнения. – Числовые ряды. – Ряды Фурье и уравнения математической физики.
	Форма промежуточной аттестации:	Зачет, экзамен

	Название:	**Дискретная математика**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-8,ОПК-2
Результаты освоения дисциплины (модуля)	**знать:**	принципы использования языка, средств, методов и моделей дискретной математики и ограничения применения изученных методов и моделей методы и модели дискретной математики, использующиеся для исследования объектов профессиональной деятельности в соответствии с профилем обучения
	уметь:	формулировать задачи на формальных языках (язык математики, языки программирования), строить мат. модели и создавать алгоритмы для компьютерных программ, реализующих поставленные профессиональные задачи

		использовать методы дискретной математики для решения практических задач в предметной области, определяемой будущей профессиональной деятельностью
	владеть навыками /иметь опыт:	анализа задач, возникающих в предметной области, связанной с направлением обучения, и их формализации с использованием методов дискретной математики применения всего арсенала методов дискретной математики, который необходим для формирования профессиональных навыков
Содержание:		Множества. Отношения. Функции. Графы. Маршруты, цепи, циклы. Связность. Графы. Алгоритмы поиска на графах. Графы. Остов графа. Фундаментальные циклы. Математическая логика. Логические исчисления. Логические функции. Формы представления логических функций и переходы между ними. Минимизация логических функций. Полные системы логических функций. Логические задачи. .
Форма промежуточной аттестации:		Экзамен

Название:		**Теория вероятностей и математическая статистика**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ОПК-2
Результаты освоения дисциплины (модуля)	**знать:**	– основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики; – основы комбинаторного анализа; – основные понятия теории автоматов; – теоретическую часть курса на уровне, обеспечивающем ориентацию в основных принципах и направлениях развития интеллектуальных информационных,
	уметь:	– применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; – выбирать математические методы и реализующие их программные средства для решения конкретных задач;
	владеть навыками /иметь опыт:	– навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; – практического умения и навыки при решении задач, сформулированных в данной рабочей программы, в различных предметных областях.
Содержание:		Основы теории вероятностей Употребление вероятностных методов в науке. Условия применимости вероятностных моделей. Различные подходы к математической формализации случайности и вероятности. Основные моменты истории развития теории вероятностей. Аксиоматика А.Н. Колмогорова. Вероятностное пространство, алгебра событий. Вероятность и ее свойства. Примеры вероятностных пространств. Конечные вероятностные пространства, классическое определение

	вероятности, урновые схемы. Условная вероятность. Независимость событий. Формула полной вероятности. Формула Байеса. Произведение вероятностных пространств. Независимые испытания Бернулли. Случайные величины. Распределение вероятностей Случайные величины. Функции распределения случайных величин. Понятие интеграла Лебега. Абсолютно непрерывные, дискретные и сингулярные случайные величины. Плотность распределения. Моменты случайных величин. Математическое ожидание, дисперсия, ковариация и их свойства. Распределение функций от случайных величин. Случайные величины, связанные с испытаниями Бернулли. Биномиальное и геометрическое распределения. Теорема Пуассона, оценка отклонения биномиальных вероятностей от пуассоновских. Неравенства Маркова и Чебышева. Закон больших чисел в форме Чебышева. Совокупности случайных величин. Совместное распределение. Независимость случайных величин. Формула свертки. Последовательности случайных величин. Виды сходимости последовательностей случайных величин: сходимость по вероятности, сходимость почти всюду, сходимость в среднем, сходимость по распределению. Связь между ними. Лемма Бореля - Кантелли. Неравенство Колмогорова. Усиленный закон больших чисел Колмогорова. Непрерывные распределения: нормальное, показательное, равномерное. Аналитические методы в теории вероятностей Аналитический аппарат теории вероятностей: производящие функции, преобразования Лапласа - Стилтьеса, характеристические функции и их свойства. Закон больших чисел в форме Хинчина. Центральная предельная теорема. Теорема Муавра - Лапласа. Условное математическое ожидание. Основы теории случайных процессов Цепи Маркова. Эргодическая теорема. Понятие случайного процесса. Пуассоновский процесс. Винеровский процесс.
Форма промежуточной аттестации:	Экзамен

Название:		**Информационные технологии**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ПК-24
Результаты освоения дисциплины (модуля)	**знать:**	– возможности современных информационных технологий; средства подготовки аналитических документов с применением информационных технологий; современные виды информационного взаимодействия и обслуживания; – назначение, функции и механизмы защиты операционных систем и баз данных; представление информации в телекоммуникационных системах и методы ее обработки; методы обработки данных, реализованные в информационно-аналитических системах для поддержки принятия решений
	уметь:	– ориентироваться в типах и видах корпоративных информационных систем; приобрести навыки анализа и выбора корпоративных информационных систем.

		– выявлять недостатки информационной системы управления предприятием
	владеть навыками /иметь опыт:	– самостоятельного усвоения новых знаний и принятия решений в области информационных технологий – принципами выбора информационных систем для решения типовых профессиональных задач
Содержание:		– самостоятельного усвоения новых знаний и принятия решений в области информационных технологий – принципами выбора информационных систем для решения типовых профессиональных задач – Введение в информационные технологии – Управление проектами. – Базы данных. – Компьютерные сети и web-технологии
Форма промежуточной аттестации:		Экзамен

Название:		**Математический аппарат и средства анализа безопасности программного обеспечения**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-2, ПСК-8.2, ПСК-8.4
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:		Экзамен

Название:		**Основы управленческой деятельности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ОПК-5, ПК-18
Результаты освоения	**знать:**	– научные основы, цели, принципы, методы и технологии управленческой деятельности; – знать основные понятия и определения теории управления;
	уметь:	– работать в коллективе, принимать управленческие решения и

		оценивать их эффективность; – 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 выбора, обоснования, реализации и контроля результатов управленческого решения; – осуществлять оценку воздействия факторов внешней среды на организацию; – осуществлять оценку сильных и слабых сторон организации.
Содержание:		Тема 1. Сущность и методологические основы управления организацией. Тема 2. История развития управленческой мысли и практики. Тема 3. Возникновение и развитие науки управления за рубежом. Тема 4. Сущность и содержание теории управления Тема 5. Системный подход в управлении Тема 6. Организационные формы и структуры управления. Тема 7. Процесс управления и его содержание. Тема 8. Методология и организация процесса разработки управленческого решения. Тема 9. Общие функции управления. Тема 10. Информационные и коммуникативные процессы в управлении. 10.1. Понятие информации. Тема 11. Эффективность процесса управления. Тема 12. Основы теории социального управления. Тема 13. Человек в системе управления. Тема 14. Система государственного управления.
Форма промежуточной аттестации:		Зачет

Название:		**Языки программирования**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-3, ПСК-8.1
Результаты освоения дисциплины (модуля)	**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	навыками работы с современными интегрированными средами

	/иметь опыт:	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 Проектирование программных алгоритмов (основные принципы и подходы). Пользовательские функции. 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:	**Технологии и методы программирования**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-8, ОПК-3, ПК-10
Результаты освоения дисциплины (модуля)	**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 ОПОП. Объектно-информационные- модели. Язык C++. Классы и объекты, поля и методы, инкапсуляция. Конструкторы и деструкторы. Шаблоны. Исключения. Модуль 4. Современные технологии программирования. ОПОП. Архитектура .NET. Язык C#. Наследование и полиморфизм. Интерфейсов базовой библиотеки классов .NET Модуль 5. Современные технологии программирования. ОПОП. Основы разработки визуального интерфейса. Язык C#. Модуль 6. Современные технологии программирования. ОПОП. Проектирование ПО. Модуль 7. Современные технологии программирования. Тестирование ПО.
	Форма промежуточной аттестации:	Зачет, экзамен

	Название:	**Основы информационной безопасности**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-5, ПК-11, ПСК-8.3
Результаты освоения дисциплины (модуля)	**знать:**	– основные информационные технологии, используемые в автоматизированных системах; сущность и понятие информации, информационной безопасности и характеристику ее составляющих; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
	уметь:	– Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
	владеть навыками /иметь опыт:	– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – навыками работы с нормативными правовыми актами; – навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; – профессиональной терминологией в области информационной безопасности;

		– навыками анализа информационной инфраструктуры государства; – навыками формальной постановки и решения задачи обеспечения информационной безопасности объекта
Содержание:		Влияние процессов информатизации общества на составляющие национальной безопасности. Национальные интересы в информационной сфере. Интересы личности. Интересы общества. Интересы государства. Угрозы национальным интересам РФ в информационной сфере. Угрозы информационному обеспечению государственной политики РФ. Угрозы безопасности информационных и телекоммуникационных средств и систем. Источники угроз ИБ РФ. Государственная информационная политика РФ. Информационные ресурсы современного общества. Государственная информационная политика РФ. Основные положения. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации. Информационные ресурсы современного общества. Информационное противоборство. Классификация угроз информационной безопасности. Различные подходы. Системная классификация и общий анализ угроз безопасности информации. Виды угроз. Происхождение угроз. Предпосылки появления угроз. Источники угроз. Модели угроз и нарушителей Классы угроз информационной безопасности в руководящих документах. Угрозы в методе CRAMM. Форс-мажорные угрозы. Организационные недостатки. Человеческие ошибки. Технические неполадки Преднамеренные действия. Угрозы информационной безопасности в документах ФСТЭК России Каналы несанкционированного получения информации. Классификация. Обычные уязвимости. Примеры уязвимостей в различных сферах безопасности: Внешняя среда и инфраструктура. Аппаратные средства. Программные средства. Система связи. Документы. Персонал. Процедурные. Обычные уязвимости обработки бизнес-приложений. Общепримененимые уязвимости. Стандарты информационной безопасности: международные; межгосударственные; государственные стандарты Российской Федерации; государственные стандарты Российской Федерации, оформленные на основе аутентичного текста международного стандарта; государственные военные стандарты Российской Федерации; стандарты отраслей, в том числе и на оборонную продукцию; стандарты предприятий. Сервисы безопасности. Аутентификация. Управление доступом. Конфиденциальность данных. Целостность. Неотказуемость. Сетевые механизмы безопасности. Администрирование средств безопасности. Администрирование сервисов безопасности Меры и средства защиты информации. Оценка проблем безопасности. Политика информационной безопасности. Средства контроля целостности. Средства контроля доступности. Средства контроля учетности, подлинности и надежности
Форма промежуточной аттестации:		Экзамен

Название:	**Криптографические методы защиты информации**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося,	

формируемые в результате освоения дисциплины (модуля):		ОК-8, ПК-14, ПК-23
Результаты освоения дисциплины (модуля)	**знать:**	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; типовые шифры с открытыми ключами; модели шифров и математические методы их исследования;
	уметь:	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять математические методы исследования моделей шифров;
	владеть навыками /иметь опыт:	криптографической терминологией; навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии
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:		**Организация ЭВМ и вычислительных систем**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-8, ПК-13
Результаты освоения дисциплины (модуля)	**знать:**	– архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; – терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; – технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; – принципы применения современных информационных технологий в науке и предметной деятельности.
	уметь:	– проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; – осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; – использовать математический аппарат и информационные технологии при изучении естественных дисциплин, работать на компьютере (использовать основных математических программ, программ отображения результатов, поиск информации через интернет, пользование электронной почтой).
	владеть навыками	– методиками оценки показателей качества и эффективности ЭВМ и

	/иметь опыт:	вычислительных систем; – навыками работы с технической документацией на ЭВМ и вычислительные системы; – методами поиска и обработки информации как вручную, так и с применением современных информационных технологий.
	Содержание:	Системы счисления. Перевод чисел из одной системы счисления в другую. Представление целых и вещественных чисел в компьютере. Введение в алгебру логики. Правила недесятичной арифметики. Принципы построения вычислительных машин. Понятия о функциональной, структурной организации и архитектуре ЭВМ. Архитектурные особенности и организация функционирования вычислительных машин различных классов. Система памяти. Процессор, основные характеристики и система команд. Вычислительные сети. Глобальная сеть WWW. Поиск информации через интернет. Язык запросов.
	Форма промежуточной аттестации:	Экзамен, зачет

	Название:	**Техническая защита информации**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОПК-8, ПК-14, ПСК-8.5
Результаты освоения дисциплины (модуля)	**знать:**	– технические каналы утечки информации; – возможности технических средств перехвата информации; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – организацию защиты информации от утечки по техническим каналам на объектах информатизации; – основы физической защиты объектов информатизации; – основные характеристики сигналов электросвязи, спектры и виды модуляции; – 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:	– анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; – пользоваться нормативными документами по противодействию технической разведке; – анализировать и оценивать угрозы информационной безопасности объекта; – 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:	– методами и средствами технической защиты информации; – методами расчета и инструментального контроля показателей

		технической защиты информации; – 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. Информация как предмет защиты. Демаскирующие признаки объектов защиты. Источники опасных сигналов. Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственно, энергетическое и структурное скрытие информации и ее носителей. Дезинформирование как метод скрытия. Комплексное применение методов защиты. Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Средства инженерной защиты и технической охраны. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источнику информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации. Физические основы защиты информации. Физические основы побочных электромагнитных излучений и наводок. Распространение сигналов в технических каналах утечки информации. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Основные направления развития технической разведки. Средства технической разведки. Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления. Генераторы линейного и пространственного зашумления. Организационные основы инженерно-технической защиты информации. 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:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-4, ОПК-6, ПК-21
Результаты освоения дисциплины (модуля)	**знать:**	– основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; – правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; – организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
	уметь:	– 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; – применять нормативные отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; – 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; – методами организации и управления деятельностью служб защиты информации на предприятии;
	Содержание:	Раздел 1. Правовое обеспечение информационной безопасности. Основы теории правового обеспечения информационной безопасности. Законодательство об информации, информационных технологиях и о защите информации. Законодательство о

	персональных данных. Законодательство в области интеллектуальной собственности. Понятия коммерческой и государственной тайн. Законодательство о коммерческой тайне, государственной тайне. Законодательство об электронной подписи. Законодательство о техническом регулировании. Правовое регулирование деятельности организация в области информационной безопасности. Система лицензирования деятельности организаций по оказанию услуг в области информационной безопасности. Система сертификации средств защиты информации. Аттестация объектов обработки конфиденциальной информации. Раздел 2. Организационное обеспечение информационной безопасности. Назначение и структура организационной защиты информации. Организация внутриобъектового режима на предприятиях. Организация пропускного режима на предприятиях. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Организация охраны предприятий. Защита информации при публикаторской и рекламной деятельности. Организация аналитической работы по предупреждению утечки конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.
Форма промежуточной аттестации:	Экзамен

Название:		**Программно-аппаратные средства обеспечения информационной безопасности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-8, ПК-10, ПК-14
Результаты освоения дисциплины (модуля)	**знать:**	Программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; Типовые архитектуры и принципы построения современных защищенных информационных систем; Угрозы и атаки, характерные для распределенных информационных систем
	уметь:	Проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы
	владеть навыками /иметь опыт:	Навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
Содержание:		Программное обеспечение для моделирования сетей передачи данных. Эмулятор GNS3. Основы работы и моделирование простых схем. Протоколы удаленного доступа. Протоколы telnet, ssh. Обеспечение безопасности при передаче данных по сети. Сравнительный анализ. Протокол настройки времени. Динамическая IP-маршрутизация. Внутренние протоколы маршрутизации. Пограничный шлюзовой протокол маршрутизации. Протоколы RIP, IGRP и EIGRP. Протокол динамической маршрутизации OSPF. Атака типа «Отказ в обслуживании» (DoS-атака). Механизмы защиты от некоторых типов DoS-атак. Антиспуфинг. Защита от IP-спуфинга.

	Защита от ARP-спуфинга. Защита внутреннего периметра сети передачи данных. Сегментация сетей передачи данных. Технология VLAN. Передача трафика между VLAN. Маршрутизация трафика между VLAN на основе коммутаторов 2-го и 3-го уровней. Технологии VTP-сервер и Port-security. Фильтрация трафика. Изучение технологии ACL (Access Control List). Типы ACL. Создание списков доступа. Общие принципы Virtual Private Network (VPN). Сравнительный анализ протоколов VPN. Настройка VPN соединения через протокол GRE. Базовые понятия и настройка WebVPN на маршрутизаторах кампании Cisco. Применение SSL VPN Базовые понятия и настройка VPN с помощью протокола IPSec на маршрутизаторах Cisco. Основы работы в ОС семейства Linux. Управление правами доступа. Администрирование пользователей. Управление файлами и каталогами. Ссылки. Архивирование и резервное копирование системы. Восстановление системы после критических сбоев из архивов. Администрирование БД MSSQL. Управление правами доступа. Архивирование и восстановление БД. Обеспечение комплексной информационной безопасности в средних и крупных сетях передачи данных. Применение межсетевых экранов и адаптивных систем обеспечения информационной безопасности. Административные меры обеспечения комплексной безопасности в информационных системах. Перспективные технологии обеспечения безопасности информации в информационных технологиях.
Форма промежуточной аттестации:	Экзамен, КП

	Название:	**Управление информационной безопасностью**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-6, ПК-12, ПК-19, ПК-28
Результаты освоения дисциплины (модуля)	**знать:**	– сущность и понятие информации, информационной безопасности и характеристику ее составляющих; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); – – основные методы управления информационной безопасностью; – методы аттестации уровня защищенности автоматизированных систем; – принципы формирования политики информационной безопасности в автоматизированных системах;
	уметь:	– анализировать и оценивать угрозы информационной безопасности объекта; – разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; – оценивать информационные риски в автоматизированных системах; – применять нормативные правовые акты и нормативные

		методические документы в области обеспечения информационной безопасности; – определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; – разрабатывать частные политики информационной безопасности автоматизированных систем; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;
	владеть навыками /иметь опыт:	– профессиональной терминологией в области информационной безопасности; – навыками работы с нормативными правовыми актами; – методами организации и управления деятельностью служб защиты информации на предприятии; – методами управления информационной безопасностью автоматизированных систем; – методами формирования требований по защите информации; – методами оценки информационных рисков;
Содержание:		Функции управления. Законы управления. Требования к управленческому решению. Понятие процесса. Понятие процессного подхода. Процессный подход к разработке, эксплуатации, анализу, сопровождению и совершенствованию СУИБ. Задание требований к информационной безопасности организации. Информационные активы. Инвентаризация и учет. Оценка рисков нарушения безопасности. Ключевые средства контроля. Разработка собственных рекомендаций. Политика информационной безопасности. Организация защиты. Инфраструктура информационной безопасности. Безопасность доступа сторонних организаций. Идентификация рисков, связанных с подключениями сторонних организаций. Условия безопасности в контрактах, заключённых со сторонними организациями. Классификация ресурсов и их контроль. Ответственность за ресурсы. Классификация информации. Безопасность персонала. Вопросы безопасности и их отражение в должностных инструкциях и при выделении ресурсов. Обучение пользователей. Администрирование компьютерных систем и вычислительных сетей. Защита оборудования. Обслуживание систем. Защита от вредоносного программного обеспечения. 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. Слежение за доступом к системам и их использованием. Разработка и сопровождение информационных систем. Требования к безопасности систем. Безопасность в прикладных системах. Защита файлов прикладных систем. Безопасность в среде разработки и рабочей среде. Вопросы бесперебойной работы организации.. Выполнение правовых требований. Проверка безопасности информационных систем.
Форма промежуточной аттестации:		Экзамен

Название:	**Инженерная графика**
Название и номер направления	10.05.03 Информационная безопасность автоматизированных систем

и/или специальности:		
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ПК-7
Результаты освоения дисциплины (модуля)	**знать:**	– основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации; – теорию и основные правила построения эскизов, чертежей, схем, нанесения надписей, размеров и отклонений, правила оформления графических изображений в соответствии со стандартами ЕСКД;
	уметь:	– применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; – читать чертежи и схемы, выполнять технические изображения в соответствии с требованиями стандартов ЕСКД, выполнять эскизирование, деталирование, сборочные чертежи, технические схемы, в том числе с применением средств компьютерной графики;
	владеть навыками /иметь опыт:	– навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации. – способами построения графических изображений, создания чертежей и эскизов, конструкторской документации, в том числе, с применением компьютерных пакетов программ.
Содержание:		Традиционные и компьютерные технологии выполнения чертежей. Требования к техническим изображениям. Метод проецирования. Состав изображения. Комплексный чертеж. Стандартные изображения - основные виды, дополнительные виды, аксонометрические изображения. Технический рисунок. Образование поверхностей и их задание на чертеже. Общий алгоритм построения линии пересечения поверхностей. Частные случаи пересечения поверхностей. Построение, обозначение, классификация сечений и разрезов. Общие правила нанесения размеров на чертеже. Предельные отклонения. Виды конструкторских документов. Чертеж общего вида. Чертеж детали, сборочный чертеж, спецификация. Стандарты ЕСКД. Основными задачами изучения дисциплины являются: развитие пространственного воображения студента, освоение теории и практики построения чертежа: основных и дополнительных видов, построение видов разрезов, сечений, линий пересечения поверхностей, чертежей деталей, узлов, сборочных чертежей.
Форма промежуточной аттестации:		Зачет

Название:		**Сети и системы передачи информации**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-8, ПК-24
Результаты освоения	**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:		**Математическая логика и теория алгоритмов**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ПК-2
Результаты освоения дисциплины (модуля)	**знать:**	основные принципы математической логики; основы исчисления высказываний; основы исчисления предикатов; формализации понятия алгоритма: машины Тьюринга, рекурсивные функции; основные понятия теории сложности алгоритмов;
	уметь:	оценивать сложность алгоритмов и вычислений; классифицировать алгоритмы по классам сложности.
	владеть навыками /иметь опыт:	способами оценки сложности работы алгоритмов навыками построения алгоритмов информационных и технических систем;
Содержание:		Логика высказываний. Логические связки. Формулы алгебры высказываний. Классификация формул. Равносильность формул. Логическое следование. Представление булевых функций формулами. Замкнутые классы. Критерии полноты систем булевых функций. Минимизация булевых функций. Приложения алгебры логики. Классификация функций К-значной логики, системы функций К-значной логики. Особенности k-значных логик. Предикаты. Операции над предикатами. Исчисления высказываний и предикатов, их полнота и непротиворечивость. Аксиоматические системы, формальный вывод. Вывод из семейства гипотез. Свойства. Непротиворечивость и полнота исчисления высказываний. Принцип резолюций для логики высказываний и логики предикатов; Независимость системы аксиом исчисления высказываний. Примеры аксиоматизаций исчисления высказываний. Реляционная алгебра и реляционное исчисление. Теория алгоритмов, структурированные программы, частично рекурсивные функции и машины Тьюринга. Алгоритмически разрешимые и неразрешимые проблемы. Понятие о сложности алгоритмов. Подходы к оценкам сложности алгоритмов.
Форма промежуточной аттестации:		Экзамен

Название:	**Аппаратные средства вычислительной техники**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-8, ПК-10, ПСК-8.1
Результаты освоения дисциплины (модуля)	**знать:**	аппаратные средства как базу для построения и развития информационных технологий, эффективно применять их для решения научно-технических и прикладных задач в соответствии с направлением профессиональной деятельности; теоретические и методические основы и понимать содержание таких предметных областей, как архитектура, организация и структурное построение компьютеров; микропроцессорные системы; многопроцессорные и параллельные вычислительные системы; вычислительные и коммуникационные сети.
	уметь:	профессионально решать задачи в процессе производственной и технологической деятельности с учетом современных достижений науки и техники, включая обоснованный выбор технических решений в области информационных и телекоммуникационных систем с учётом существующих и вновь разрабатываемых средств аппаратной поддержки.
	владеть навыками /иметь опыт:	навыками оценки производительности подсистем и компонент ЭВМ, а так же ЭВМ в целом; иметь навыки настройки и оптимизации работы аппаратного обеспечения ЭВМ; теоретическими знаниями об архитектуре IBM PC - совместимого компьютера и организации основных его частей; владеть знаниями о современных технических характеристиках аппаратного обеспечения ЭВМ.
Содержание:		История развития ЭВМ. Архитектура и алгоритм работы современного компьютера. История развития и архитектура современных. Организация оперативной памяти. Организация системы охлаждения ЭВМ. Организация материнской платы персонального компьютера. Шины ЭВМ. Видеоподсистема и организация вывода информации на экран. Современные носители данных. Иерархия запоминающих устройств ЭВМ. Организация подсистемы электропитания персонального компьютера.
Форма промежуточной аттестации:		Зачет

Название:		**Гуманитарные аспекты информационной безопасности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-5, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	– основные стандарты, регламентирующие управление ИБ; – принципы работы процессов управления ИБ; – подходы к интеграции СУИБ в общую систему управления предприятием;
	уметь:	– анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ; – определять цели и задачи решаемые разрабатываемыми процессами управления ИБ; – применять процессный подход к управлению ИБ в различных

		сферах деятельности; – используя современные методы и средства, разрабатывать процессы управления ИБ, учитывающими особенности функционирования предприятия и решаемых им задач и оценивать их эффективность;
	владеть навыками /иметь опыт:	терминологией и процессным подходом построения систем ИБ; навыками анализа активов организации, их угроз и уязвимости в рамках области деятельности СУИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
Содержание:		Изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта
Форма промежуточной аттестации:		Зачет

Название:		**Основы деловой и научной коммуникации**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-7, ОПК-5, ПК-7
Результаты освоения дисциплины (модуля)	**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:	**Социология организаций и организационное поведение**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-6, ОПК-4

Результаты освоения дисциплины (модуля)	**знать:**	• основные модели организационного поведения и их характеристики; • подходы к определению организационной эффективности, их достоинства и ограничения; • основные характеристики личности, группы и организации, влияющие на поведение.
	уметь:	• анализировать поступки людей, понимать причины поведения; • организовать групповую работу; • выбирать адекватные средства для общения; • показать возможности управления поведением людей на практических примерах.
	владеть навыками /иметь опыт:	• навыками предсказания поведения работника в будущем; • навыками управления поведением людей.
Содержание:		1.Теория организации. 2. Организационное поведение.
Форма промежуточной аттестации:		Зачет

Название:		**Электроника и схемотехника**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ОПК-8, ПК-10
Результаты освоения дисциплины (модуля)	**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. Полупроводниковые приборы. Свойства p-n перехода. Диоды, стабилитроны, Выпрямление и стабилизация напряжения. Ограничение сигналов. Биполярный транзистор. Принцип работы, схемы включения БТ. Усиление электрических сигналов. Полевой транзистор. Схемы включения ПТ. Усилители на ПТ. Схемы замещения, параметры и характеристики полупроводниковых приборов. Электронные усилители. Принципы электронного усиления. Режимы работы усилительных элементов. Двухкаскадные усилители. Дифференциальные усилители. Схемы замещения, параметры и характеристики. Обратная связь в усилителях. Структурная схема усилителя с ОС. Определение исходных параметров и петлевой передачи. 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. Аналоговые компараторы напряжений. Устройство и принцип действия. Характеристики аналоговых компараторов. Классификация компараторов. Применение аналоговых компараторов. Активные фильтры. 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, КР

	Название:	**Защита информации в предпринимательской деятельности**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОПК-6, ПК-6, ПК-19
Результаты освоения дисциплины (модуля)	**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. Система конфиденциальной информации фирмы. Принципы и методы защиты коммерческой информации Минимизация предпринимательского риска и защита информации при совершении сделок. Обеспечение защиты интеллектуальной собственности. Особенности защиты информации в чрезвычайных ситуациях Организация защиты информации при работе с кадрами.
	Форма промежуточной аттестации:	Зачет соценкой

Название:		**История становления систем информационной безопасности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-3, ОК-5, ОПК-4
Результаты освоения дисциплины (модуля)	**знать:**	о критериях, которым должно соответствовать информационное общество, о соответствии современного общества этим критериям.
	уметь:	Периоды развития общества, этапы развития вычислительной техники, критерии периодизации, развитие элементной базы, ведущих ученых в этой области, развитие отечественной вычислительной техники
	владеть навыками /иметь опыт:	Проводить поиск информации по требуемой тематике, аргументировано и последовательно излагать свое мнение, проводить сравнительный анализ экономического состояния общества и вычислительной техники.
Содержание:		Появление понятия «информационное общество». Критерии информационного общества, согласно различным авторам. Информационные структуры. Появление понятия «информационное общество». Критерии информационного общества, согласно различным авторам. (Т. Стоуньер, Д. Белл, А. И. Ракитов, И.Н. Курносов) Информационные структуры. Этапы развития вычислительной техники. Критерии периодизации. Поколения. Характерные признаки Первый этап. Возникновение счета в человеческом обществе. Древнейшие виды счета, распространение и развитие. Счет, использующий перекладывание предметов. Возникновение позиционного счета. Абак, его разновидности. Этапы развития вычислительной техники. Критерии периодизации. Поколения. Характерные признаки Счет, использующий перекладывание предметов. Возникновение позиционного счета. Абак, его разновидности. Абак в России. Теории возникновения. Создание рабдологии (изобретение палочек Непера). Жизнь, научная и изобретательская деятельность Джона Непера Двоичная система Два направления усовершенствования палочек Непера. Работы Женейема и Люка, “Математический орган” Кирхера и Шотта. Вариант механизации палочек Непера Самюэлем Морлендом. Другие варианты механизации палочек Непера. (Грийе,Пти, Лейпольд). Рабдология. Деятельность Непера. Двоичная система. Направления усовершенствования изобретений Непера. Таблицы логагифмов. Изобретение аналогового вычислительного устройства. Развитие логарифмической линейки, разновидности. Появление таблиц логарифмов. Логарифмические шкалы. Шкала Гюнтера. Изобретение логарифмической линейки. Проблемы авторства. Усовершенствования логарифмической линейки. Ее разновидности. Машина Паскаля (“Паскалево колесо”). Механическая вычислительная машина Вильгельма Шиккарда. Работы Самюэля Морленда, Клода Перро, Родригеса Перейры. Теория и практика зубчатого зацепления (использование в суммирующих машинах). Клавишные суммирующие машины. Суммирующие машины в России. Начало второго, механического, этапа развития. Создание суммирующих машин. Принципы работы, виды, используемые

	зацепления. Деятельность выдающихся изобретателей. Создание арифмометров. Деятельность российских ученых. Промышленный выпуск. Создание арифмометров “Арифметический инструмент” Готфрида Вильгельма Лейбница, Арифмометр Чебышева. Американская компания арифмометров. Промышленный выпуск. Создание разностных машин. Принципы работы. Жизнь и деятельность Чарльза Бэббиджа. Изобретение и создание разностной и аналитической машин. Разностные машины других авторов. Вклад Бэббиджа в развитие вычислительной техники Создание разностных машин. Принципы работы. Деятельность Чарльза Бэббиджа. Изобретение и создание разностной и аналитической машин. Вклад Бэббиджа в развитие вычислительной техники. Ада Лавлейс. Возникновение программирования. Осознание возможностей вычислительной техники Начало электромеханического этапа. Табулятор Голлерита. Деятельность Говарда Гатуэя Айкена. Создание машин “Марк 1”; “Марк II”. Работы К. Цузе. Машины “Ц1”,”Ц2”, ”Ц3”, ”Ц4”. Работы Джорджа Штибитца. Машины “Модел 1-5” (Фирма “Белл”). Создание РВМ-1 (Бессонов). Начало создания электромеханической вычислительной техники. Релейные вычислительные машины. Отечественная релейная вычислительная техника. Область применения. Конкурентоспособность. Создание электронной вычислительной техники. Значение работ Неймана. Проблемы авторства. Процесс создания языков программирования Создание машины ЭНИАК (Моучли, Эккерт). Работы Атанасова. Проблемы авторств. Жизнь и деятельность Джона фон Неймана.
Форма промежуточной аттестации:	зачет

Название:		**Системный анализ объектов обработки данных**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-1, ПК-8
Результаты освоения дисциплины (модуля)	**знать:**	методы и приемы теории и практики системного исследования объектов анализа различной природы; оценивать полученную при анализе информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа;
	уметь:	выполнять системное описание объекта анализа, обоснованно выбирать интегральный критерий и систему ограничений; применять физико-математические методы для решения критериальных практических задач по системному анализу хорошо структурированных систем с применением стандартных программных средств; анализировать физическое содержание процессов в системе и выбирать рациональные решения для минимизации влияния имевшихся проблем;
	владеть навыками /иметь опыт:	навыками критического восприятия информации на всех этапах алгоритма действий от обнаружения проблемы до принятия оптимального решения
Содержание:		Цели курса. Системный анализ, определение. Системы, проблемы, цели, задачи. Этапы системного анализа. Выбор как задача

	оптимизации. Использование теории графов. Анализ данных. Способы передачи данных. Физико-математические методы для решения критериальных практических задач по системному анализу
Форма промежуточной аттестации:	Зачет с оценкой

	Название:	**Иностранный язык (технический перевод)**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОК-7, ОПК-4, ПК-1
Результаты освоения дисциплины (модуля)	**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 языкам 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.
Форма промежуточной аттестации:		Зачет

Название:	**Разработка и эксплуатация защищенных автоматизированных систем**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины	ОПК-4, ПК-9, ПК-20

(модуля):		
Результаты освоения дисциплины (модуля)	**знать:**	– основные информационные технологии, используемые в автоматизированных системах; – основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); – автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
	уметь:	– разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; – восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;
	владеть навыками /иметь опыт:	– навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем; – навыками анализа основных узлов и устройств современных автоматизированных систем; – навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; – методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; – навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
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. Настройка регистрации системных 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:	**Безопасность операционных систем**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ОПК-3, ПК-11, ПК-22
Результаты освоения дисциплины (модуля)	**знать:**	– принципы построения и функционирования, примеры реализаций современных операционных систем; – функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной – памятью, устройствами; – критерии оценки эффективности и надежности средств защиты операционных систем; – принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; – основные информационные технологии, используемые в автоматизированных системах; – возможности, классификацию и область применения макрообработки; – показатели качества программного обеспечения;
	уметь:	– использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; – оценивать эффективность и надежность защиты операционных систем; – планировать политику безопасности операционных систем;

		проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;
	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. Прикладные операционные среды. Совместимость операционных систем. Виды совместимости. Языковая и двоичная совместимость. Эмуляция. Виртуальные машины и операционные среды. Загрузка операционных. 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 многопрограммной многопользовательской ОС с графическим интерфейсом. 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, КП,

Название:		**Безопасность сетей ЭВМ**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-3, ПК-13, ПК-27
Результаты освоения дисциплины	**знать:**	– принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; – основные протоколы компьютерных сетей; – последовательность и содержание этапов построения компьютерных сетей; – эталонную модель взаимодействия открытых систем; – основные термины и понятия архитектуры компьютерных сетей.

		– методы построения и анализа эффективности применения компьютерных сетей: – принципы организации взаимодействия абонентских систем в составе современных и перспективных компьютерных сетей. – современное положение на рынке аппаратных и программных средств организации компьютерных сетей
	уметь:	– проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; – эффективно использовать различные методы и средства защиты информации для компьютерных сетей; – проводить мониторинг угроз безопасности компьютерных сетей; – организовывать и конфигурировать компьютерные сети, строить и анализировать модели компьютерных сетей, эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач
	владеть навыками /иметь опыт:	– 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; – навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности; – навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей; – навыками проектирования и настройки систем передачи данных; – навыками описания тактико-технических характеристик систем передачи данных.
	Содержание:	Основные понятия системы передачи данных. Концепция сети. Локальные вычислительные сети, расширение компьютерных сетей. Назначение компьютерной сети. Принтеры и другие периферийные устройства. Одноранговые сети, размеры сети, стоимость сети, операционные системы, реализация, целесообразность применения. Сети на основе сервера, специализированные серверы, значение программного обеспечения. 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. Коммутация и маршрутизация в сетях ЭВМ. Понятие о коммутируемой транспортной сети. Методы коммутации, их достоинства и недостатки. Коммутация цепей (линий). Коммутация сообщений. Коммутация пакетов. Принципы пакетной передачи данных. Коммутация символов. Понятие о маршрутизации сообщений, пакетов, символов. Цели маршрутизации. Основные способы маршрутизации: централизованная, распределенная, смешанная. Эффективность алгоритмов маршрутизации. Методы маршрутизации: простая, случайная, лавинная, фиксированная, адаптивная маршрутизации и их варианты. Маршрутизация пакетов. Фильтрация пакетов. Понятие маршрутизатора. Локальные и глобальные вычислительные сети. Основные понятия и определения ЛВС. Основные области и направления применения ЛВС. Типы и характеристики ЛВС. Признаки классификации ЛВС.

	Протоколы передачи данных (ППД) и методы доступа к передающей среде (МД) в ЛВС. Методы доступа Ethernet, Token Ring, Arcnet и их характеристики. Сетевое оборудование ЛВС. Сетевые адаптеры. Концентраторы (хабы). Приемопередатчики (трансиверы) и повторители (репитеры). Мосты и шлюзы. Маршрутизаторы (роутеры). Коммутаторы. Модемы и факс-модемы. Анализаторы ЛВС и сетевые тестеры. Программное обеспечение ЛВС. Особенности и структура ПО. Характеристика сетевых ОС. Способы управления ЛВС. Основные понятия и определения ГВС. Принципы организации ГВС. Системы сетевых коммуникаций. Электронная почта (ЭП). Стандарты ЭП. Адресация в Интернет. Характеристика сети Интернет. Протоколы сети Интернет. Типы сервисов Интернет. Клиентское программное обеспечение сети Интернет.
Форма промежуточной аттестации:	Экзамен, КР

Название:		**Безопасность систем баз данных**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОК-8, ОПК-8,ПК-13
Результаты освоения дисциплины (модуля)	**знать:**	принципы построения и функционирования, конфигурирования баз данных; физическую организацию баз данных, архитектуру систем баз данных; основы реляционной алгебры и SQL; средства обеспечения целостности данных; подсистемы безопасности данных в СУБД; стандарты безопасности данных.
	уметь:	отображать предметную область на конкретную модель данных; нормализовывать отношения при проектировании реляционной базы данных; создавать объекты базы данных; выполнять запросы к базе данных с использованием встроенных языков (SQL и т.п.); разрабатывать политики информационной безопасности для администрирования баз данных; анализировать, подбирать и применять эффективные средства обеспечения безопасности баз данных.
	владеть навыками /иметь опыт:	навыками разработки баз данных с учетом требований по обеспечению информационной безопасности; развертывания сервера СУБД и конфигурирования его работы; организации удаленного доступа к серверу базы данных; навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности; использования программных средств системного и прикладного назначения (СУБД, ОС), языки и системы программирования для решения профессиональных задач по обеспечению безопасности баз данных.
Содержание:		Общие принципы построения баз данных: реляционная, иерархическая и сетевая модели; распределенные базы данных в сетях ЭВМ; общая характеристика, назначение и возможности систем управления базами данных (СУБД); языковые средства СУБД; оптимизация производительности и характеристик доступа к базам

	данных; средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, языковые средства разграничения доступа, концепция и реализация механизма ролей, организация аудита событий в системах баз данных; средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, средства создания резервных копии и восстановления баз данных, технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных; нормативные документы (стандарты, регламенты, инструкции), необходимые для управления базами данных и пользователями баз данных
Форма промежуточной аттестации:	зачет, КР, экзамен,

Название:		**Обеспечение безопасности финансовой и банковской деятельности**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-12, ПК-19, ПСК-8.3
Результаты освоения дисциплины (модуля)	**знать:**	– структуру и принципы создания, внедрения и функционирования кредитно-финансового учреждения и системы ИБ в нем. – основные требования законодательства, включая отраслевые стандарты, связанные с банковской, финансовой деятельностью и обеспечением защиты обрабатываемых данных в процессе этой деятельности. – подходы к построению системы обеспечения ИБ кредитно-финансового учреждения. – положения типовых методик оценки рисков нарушения ИБ. – основные подходы к проектированию системы менеджмента ИБ кредитно-финансовой организации. – требования к эффективному использованию системы мониторинга и аудита процессов обеспечения ИБ. правила подбора, приема и увольнения сотрудников в банковском секторе, квалификационные требования к отдельным должностям.
	уметь:	– проводить оценку соответствия организации требованиям нормативных документов и стандартам по информационной безопасности – планировать мероприятия по защите коммерческой тайны и другой конфиденциальной информации в финансовом и банковском секторе. – 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 базами данных и информационно-аналитическими системами.

		– навыками работы с программными средствами обеспечения информационной безопасности. – навыками анализа и подготовки содержания разрешительно-распорядительных документов и инструкций для поддержки безопасной работы банков и финансовых организаций. – подготовки кратких аналитических обзоров по вопросам обеспечения информационной безопасности, в том числе с применением технологий Data Mining.
Содержание:		Сущность финансовой безопасности как подсистемы экономической безопасности банковской деятельности. Структура коммерческого банка. Экономическое содержание и особенности обеспечения безопасности банковской деятельности. Банковское законодательство. Регуляторы безопасности и функционирования банковской системы. Понятие и состав конфиденциальной банковской информации. Оценка возможностей предотвращения угроз финансовой безопасности в банковской системе. Угрозы безопасности банковских информационных систем. Службы защиты. Классификация и характеристика основных методов защиты информации в компьютерных системах кредитно-финансового учреждения. Безопасные протоколы информационного взаимодействия с клиентами и партнерами. Методы сбора доказательной базы и организация внутреннего расследования инцидентов. Механизмы анализа рисков и управления инцидентами.
Форма промежуточной аттестации:		Зачет

Название:		**Проектирование защищенных баз данных**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-9, ПК-13, ПСК-8.3
Результаты освоения дисциплины (модуля)	**знать:**	• угрозы безопасности баз данных; • функции современных систем управления базами данных; • архитектуру информационных систем; • основные модели данных; • последовательность и содержание этапов проектирования баз данных с учетом требований безопасности; • методологии процесса моделирования бизнес-процессов; • языки управления данными в СУБД, типы используемых данных в базах, встроенные функции; • стандарты и законодательство в сфере защиты данных.
	уметь:	• выделять сущности и связи предметной области; • формализовать поставленную задачу по обеспечению защиты баз данных; • создавать диаграммы, моделирующие информационную систему в специализированных графических редакторах на базе известных нотаций и стандартов; • разрабатывать базы данных и выполнять запросы к базе данных на базе SQL и т.п.; • разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
	владеть навыками	• методами и средствами выявления угроз безопасности в базах данных, автоматизированных системах;

	/иметь опыт:	• использования CASE-средств в проектировании; • иметь опыт составления запросов для манипулирования данными в базе, создания скриптов; • навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.
	Содержание:	Основы организации, хранения и защиты данных, основные руководящие и нормативные документы по защите информации в базах данных, методы обеспечения защиты баз данных на уровне СУБД и ОС, использование триггеров, сохраненных процедур и функции, определение правил доступа к данным, проектирование реляционных баз данных в защищенном исполнении.
	Форма промежуточной аттестации:	**Экзамен**

	Название:	**Технические средства охраны**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ПК-24, ПК-25, ПСК-8.2
Результаты освоения дисциплины (модуля)	**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 объектов информатизации**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ПК-3, ПК-23, ПК-25, ПСК-8.3
Результаты освоения дисциплины	**знать:**	• виды, источники и носители защищаемой информации; • основные угрозы безопасности информации в ОИ; • концепцию комплексной защиты информации; • основные принципы и методы комплексной защиты информации; • основные руководящие и нормативные документы по

		инженерно-технической защиты информации; порядок организации инженерно-технической защиты информации;
	уметь:	• выявлять угрозы защите информации; • описывать (моделировать) объекты защиты и угрозы безопасности информации; • применять наиболее эффективные методы и средства комплексной защиты информации в ОИ; контролировать эффективность мер комплексной защиты информации в ОИ
	владеть навыками /иметь опыт:	• оценки параметров и характеристик комплексной защиты информации в ОИ; • обучение персонала средствам комплексной защиты информации в ОИ.
Содержание:		Принципы организации и этапы разработки КОЗИОИ, а также выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов НСД к информации. Определение компонентов и условий функционирования КОЗИОИ. Материально техническое и нормативно-методическое обеспечение КСЗИ. Принципы и методы планирования функционирования КОЗИОИ. Характеристика подходов, методов и моделей к оценке эффективности систем.
Форма промежуточной аттестации:		Экзамен, КП

Название:		**Верификация безопасности информационных систем**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-2, ПК-15, ПСК-8.2
Результаты освоения дисциплины (модуля)	**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 безопас-

		ности 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:		Основные методы верификации аппаратуры и программного обеспечения – тестирование, имитационное моделирование, дедуктивный анализ, верификация моделей. Преимущества метода верификации моделей. Алгоритмические и комбинаторные трудности применения метода верификации моделей. Моделирование схем. Системы переходов. Представление систем переходов формулами логики предикатов первого порядка. Синхронные и асинхронные схемы. Формальные языки спецификации моделей. Построение модели автомата (протокола, управляющего алгоритма) на языках описания моделей программ (SMV, Promela). Двоичные разрешающие диаграммы (BDD). Алгоритм редукции BDD к каноническому виду (ROBDD). Выполнение операций над ROBDD: унарные и бинарные Булевы операции, операция ITE (мультплексорная функция от трех переменных), квантификация, проверка выполнимости, подсчет числа единиц. Эффективная машинная реализация ROBDD на основе хэш-таблиц. Общие представления о сложности в классе ROBDD (зависимость сложности от порядка переменных, сложность умножения целых чисел). Реализация алгоритмов работы с ROBDD на примере одного из распространенных пакетов (CUDD, ABCD, и др.). Алгоритм DPLL. Обоснование корректности и сложности табличного алгоритма верификации моделей. Проблема “комбинаторного взрыва”. Представления неподвижной точки. Алгоритм символьной верификации моделей. Особенности реализации алгоритма: учет ограничений справедливости, расщепленные отношения переходов, рекомбинация произведений. Табличная верификация моделей для PLTL. Верификации простых моделей с использованием системы SPIN: описание моделей, формальное задание спецификаций, проверка выполнимости спецификаций.
Форма промежуточной аттестации:		Зачет с оценкой

Название:		**Анализ безопасности протоколов**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-6, ПК-16, ПСК-8.4
Результаты освоения дисциплины (модуля)	**знать:**	методы анализа и тестирования протоколов; подходы к испытанию средств криптографической защиты и требования к встраиванию криптосистем в информационные системы;
	уметь:	разрабатывать модели нарушителя и угроз для информационных систем, выделять подсистемы и модули, содержащие критическую

		информацию; создавать формальное описание протоколов с целью их дальнейшего анализа;
	владеть навыками /иметь опыт:	методами и средствами поиска уязвимостей, анализа и верификации протоколов; общими подходами к испытанию систем криптографической защиты (аутентификация, защита данных); типовыми средствами анализа сетевых протоколов;
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:		**Проектирование технических средств и систем в защищенном исполнении**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-2, ПК-4, ПК-8, ПСК-8.3
Результаты освоения дисциплины (модуля)	**знать:**	- основные понятия, используемые при обеспечении информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении; - взаимосвязь обеспечения информационной безопасности с технологиями проектирования и создания (модернизации) объектов информатизации; - средства видов обеспечений компьютерной системы, подлежащие разработке при проектировании, создании (модернизации) компьютерной системы; - основные мероприятия по организации разработке средств видов обеспечения компьютерной системы, отвечающих требованиям информационной безопасности; - общие требования к технологической безопасности средств программного и информационного обеспечений компьютерных систем; - структуру и содержание программы обеспечения информационной безопасности проектирования, создания (модернизации)

		компьютерных систем в составе объектов информатизации; - требования к разработке средств основных видов обеспечения компьютерной системы в защищенном исполнении; - требования по обеспечению информационной безопасности стенда для разработки средств программного и информационного обеспечения; - требования информационной безопасности к документации на объекты информатизации на базе компьютерных систем; - структуру, цели создания, назначение и основные функции системы обеспечения информационной безопасности проектирования, создания (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении;
	уметь:	- определять основные мероприятия по организации разработки средств видов обеспечения компьютерной системы; - разработать требования к технологической безопасности средств программного и информационного обеспечения; - разрабатывать структуру и отдельные разделы программы обеспечения информационной безопасности проектирования, создания (модернизации) компьютерной системы в защищенном исполнении в составе объекта информатизации; - разрабатывать документы, регламентирующие обеспечение информационной безопасности разработки объектов информатизации на базе компьютерных систем в защищенном исполнении;
	владеть навыками /иметь опыт:	работы с нормативными правовыми документами в области информационной безопасности; -разработки (формирования) требований информационной безопасности к объектам и субъектам деятельности по проектированию, созданию (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении;
Содержание:		Введение в обеспечение информационной безопасности проектирования, создания, модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении. Проектирование, создание, модернизация объектов информатизации на базе компьютерной системы в защищенном исполнении как объект обеспечения информационной безопасности. Проектирование, создание, модернизация объектов информатизации на базе компьютерной системы в защищенном исполнении как объект обеспечения информационной безопасности. Требования к документации на объект информатизации на базе компьютерной системы в защищенном исполнении и на его составные части, выполнение которых обеспечивает информационную безопасность разработки этих объектов и их составных частей. Система обеспечения информационной безопасности разработки ОИ на базе компьютерной системы в защищенном исполнении.
Форма промежуточной аттестации:		Экзамен, КП

Название:	**Мониторинг безопасности информационных систем**
Название и номер направления и/или специальности:	**10.05.03 Информационная безопасность автоматизированных систем**
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	**ПК-11, ПК-17, ПК-27, ПСК-8.5**

Результаты освоения дисциплины (модуля)	**знать:**	– принципы построения современных систем обеспечения информационной безопасности; – принципы статистического анализа; – способы описания поведения систем; – типовые архитектуры и принципы построения современных защищенных информационных систем; – 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;
	уметь:	– формализовать задачу контроля параметров безопасности информационными системами; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; – 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:	– средствами фиксации параметров безопасности информационных систем; – методами реализации и верификации моделей контроля и управления доступом; – 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. Информация как предмет защиты. Демаскирующие признаки объектов защиты. Источники опасных сигналов. Методы инженерно-технической защиты информации. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственно, энергетическое и структурное скрытие информации и ее носителей. Дезинформирование как метод скрытия. Комплексное применение методов защиты. Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Средства инженерной защиты и технической охраны. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источнику информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства инженерной защиты и технической охраны. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны. Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные

	технические каналы утечки информации. Технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки. Физические основы защиты информации. Физические основы побочных электромагнитных излучений и наводок. Распространение сигналов в технических каналах утечки информации. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Характеристика технической разведки. Классификация технической разведки по видам носителя информации и средств разведки. Характеристика технической разведки. Возможности видов технической разведки по добыванию разведывательной информации. Основные направления развития Средства технической разведки. Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления. Генераторы линейного и пространственного зашумления. Организационные основы инженерно-технической защиты информации. 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.
Форма промежуточной аттестации:	Экзамен

Название:		**Администрирование средств защиты информации в компьютерных системах и сетях**
Название и номер направления и/или специальности:		**10.05.03 Информационная безопасность автоматизированных систем**
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		**ПК-26, ПК-27, ПСК-8.5**
Результаты освоения дисциплины (модуля)	**знать:**	основы администрирования подсистемы информационной безопасности распространенных операционных систем; основы администрирования вычислительных сетей; принципы и методы противодействия несанкционированному информационному воздействию на компьютерные системы и системы передачи информации; принципы организации информационных систем в соответствии по требованиям безопасности 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; администрировать подсистему информационной безопасности в компьютерных системах и сетях

	владеть навыками /иметь опыт:	навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз информационной безопасности в компьютерных системах и сетях; формирования комплекса мер по защите информации в компьютерных системах и сетях; подбора средств защиты по требованиям безопасности информации.
Содержание:		Понятие администрирования. Основные угрозы безопасности информации в компьютерных системах и сетях. Основы администрирования подсистемы информационной безопасности ОС Microsoft Windows. Основы администрирования подсистемы информационной безопасности ОС Linux. Средства защиты информации от вредоносного ПО. Средства защиты информации от несанкционированного доступа. Защита информации в сетях компьютерных
Форма промежуточной аттестации:		Зачет

Название:		**Защита информации в процессе документооборота организации**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-7, ПК-21, ПК-24, ПСК-8.2
Результаты освоения дисциплины (модуля)	**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, КР

Название:	**Элективные дисциплины по физической культуре и спорту**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате	ОК-9

освоения дисциплины (модуля):		
Результаты освоения дисциплины (модуля)	**знать:**	• научно-практические основы физической и профессионально-прикладной физической культуры; • 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. • использовать приобретенные знания и умения в практической деятельности и повседневной жизни для: повышения работоспособности, сохранения и укрепления здоровья; подготовки к профессиональной деятельности и службе в Вооруженных Силах Российской Федерации; организации и проведения индивидуального, коллективного и семейного отдыха и при участии в массовых спортивных соревнованиях
	владеть навыками /иметь опыт:	• средствами и методами укрепления индивидуального здоровья, физического самосовершенствования; • ценностями физической культуры личности для успешной социально-культурной и профессиональной деятельности.
Содержание:		1) Развитие общей выносливости 2) Прикладная физическая подготовка 3) Развитие специальной выносливости 4) Прикладная физическая подготовка 5) Прикладная физическая подготовка
Форма промежуточной аттестации:		Зачет, экзамен
Название:		**Алгоритмы направленного перебора**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-10, ПК-20, ПСК-8.1
Результаты освоения дисциплины	**знать:**	Основы алгоритмизации, алгоритмы полного перебора, приближённые алгоритмы, методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; современные средства разработки и анализа программного обеспечения на языках высокого уровня.
	уметь:	Применять изученные алгоритмы для решения прикладных задач выбирать необходимые инструментальные средства для раз- работки программ в различных операционных системах и средах;

		составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня.
	владеть навыками /иметь опыт:	методами анализа и формализации информационных процессов объекта и связей между ними; владеть профессиональной терминологией. Навыками постановки задачи и выбору путей её решения на основании полученных знаний и умений. Навыками применения соответствующих алгоритмов для решения поставленных задач.
Содержание:		Организация полного перебора. Построение дерева решений. Способы обхода дерева решений сокращение числа необходимых для решения подзадач: отсев возможных вариантов ветвления. Функции ветвления. Приближенные алгоритмы. Основные понятия. Приближенный жадный алгоритм для задачи о коммивояжере. Приближенный жадный алгоритм для задачи о рюкзаке. Приближенный жадный алгоритм для задачи о суммах элементов подмножеств. Приближенный жадный алгоритм для задачи о раскраске графа. Приближенные алгоритмы с гарантированной оценкой точности. Задача об упаковке в контейнеры. Задача распределения работ на конечное число одинаковых процессоров
Форма промежуточной аттестации:		Экзамен

Название:		**Комбинаторные алгоритмы**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-10, ПК-20, ПСК-8.1
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 пароля. 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:	Экзамен

Название:		**Нормативно-распорядительная документация в сфере обеспечения безопасности государства**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-6, ПК-1, ПСК-8.2
Результаты освоения дисциплины (модуля)	**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:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ОПК-6, ПК-1, ПСК-8.2
Результаты освоения дисциплины (модуля)	**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:		Телекоммуникационное право как суботрасль информационного права. Телекоммуникационные правоотношения. Управление в области телекоммуникаций. Система органов связи. Лицензирование деятельности в области оказания услуг связи. Сертификация средств связи. Правовое регулирование услуг телефонной связи. Правовое регулирование услуг связи по передаче данных. Правовое регулирование услуг телеграфной связи. Электронная подпись и электронная торговля. Правовой режим электронного документооборота. Правовое регулирование теле-и радиовещания. Правовое регулирование деятельности, связанной с использованием глобальной информационно-телекоммуникационной сети «Интернет». Порядок осуществления государственного надзора в области связи. Законодательство в области телекоммуникаций стран СНГ. Защита прав пользователей услугами связи. Ответственность за нарушение законодательства в области телекоммуникаций
Форма промежуточной аттестации:		Зачет

Название:	**Особенности аттестации объектов информатизации**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-16, ПК-17, ПСК-8.5
Результаты освоения дисциплины (модуля)	**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:		Экзамен

Название:	**Анализ рисков информационной безопасности**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате	ПК-16, ПК-17, ПСК-8.5

	освоения дисциплины (модуля):	
Результаты освоения дисциплины (модуля)	**знать:**	– сущность и понятие информации, информационной безопасности и характеристику ее составляющих; – источники и классификацию угроз информационной безопасности; – способы описания поведения систем; – угрозы и атаки, характерные для распределенных информационных систем; – место анализа рисков в общей системе обеспечения информационной безопасности; – основные положения отечественных и зарубежных стандартов по риск-менеджменту и оценке рисков информационной безопасности
	уметь:	– анализировать и оценивать угрозы информационной безопасности объекта; – - оценивать информационные риски в автоматизированных системах; – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; – контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; – разрабатывать методы и средства для проверки выполнения требований информационной безопасности и поиска уязвимостей
	владеть навыками /иметь опыт:	– профессиональной терминологией в области информационной безопасности; – навыками работы с нормативными правовыми актами; – методиками оценки рисков информационной безопасности; – навыками применения средств анализа безопасности информационных систем;
	Содержание:	Понятие риска в различных сферах жизни общества. Взаимосвязь основных понятий в области оценки рисков. Место анализа рисков в общей схеме управления ИБ. Подходы к оценке рисков ИБ: качественный, количественный. Экономическая модель оценки рисков. Вероятностная модель оценки рисков. Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010. Методы оценки риска. ГОСТ Р ИСО 27005. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ. Методики и программное обеспечение для оценки рисков ИБ. Метод анализа и управления рисками CRAMM. Средство оценки рисков Microsoft Security Assessment Tools. Оценка критичных угроз, активов и уязвимостей OCTAVE. Средство качественной оценки vsRisk. Средство количественной оценки рисков Practical Threat Analysis. Методика RiskWatch. Методика управления рисками Microsoft The Security Risk Management Guide. Средство оценки рисков R-VisionRiskManager. Принятие решений по результатам оценки рисков. Политика обработки рисков. Подведение итогов
	Форма промежуточной аттестации:	Экзамен

Название:	**Принятие решений и оценка рисков в сфере информационной безопасности**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-5, ПК-22, ПСК-8.4
Результаты освоения дисциплины (модуля)	знать:	общую методологию и схему процесса выработки решений, в том числе в условиях неопределенности и риска, конфликта; формальные методы и процедуры измерения предпочтений ЛПР для построения функций выбора наилучших альтернатив; основы экспертных методов; технологии оценки эффективности и предпочтительности альтернатив по выбранным критериям в сложных ситуациях.
	уметь:	применять методы дискретной математики, оптимизации, теории игр в задачах, связанных с принятием решений использовать основные положения теории выбора и принятия решений (законы, принципы, методы) в практической работе; организовывать процедуру экспертной оценки для выработки решения по поставленной проблеме группой экспертов. формализовать проблемы выбора и принятия решений в сфере информационной безопасности; 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:	формализации содержательных задач принятия решений и оценки риска; выбора модели, метода для решения задач принятия решений и оценки риска в сфере информационной безопасности
	Содержание:	Основные понятия исследования операций и системного анализа. Методологические основы теории принятия решений. Бинарные отношения как способ описания системы предпочтений ЛПР. Методы многокритериальной оптимизации . Метод аналитической иерархии (AHP). Принятие решений в условиях полной неопределенности, риска и конфликта. Экспертные методы. Понятие и структура экспертной системы. Разработка и применение экспертных систем. Инженерия знаний. Основные понятия инженерии знаний. Программные системы поддержки принятий решений. Интеллектуальный анализ данных (Data Mining), основные методы и алгоритмы.
	Форма промежуточной аттестации:	Зачет

	Название:	**Исследование операций**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-5, ПК-22, ПСК-8.4
Результаты освоения дисциплины (модуля)	**знать:**	основные разделы исследования операций и решаемые в них задачи, методику проведения исследования операций, методы отыскания оптимальных решений в разных классах задач исследование операций
	уметь:	строить математическую модель задачи, подбирать метод ее решения, находить оптимальное решение и делать содержательную интерпретацию.
	владеть навыками /иметь опыт:	терминологией исследования операций и соответствующим математическим аппаратом.

Содержание:	Общие вопросы ИО. Календарное планирование программ сетевыми методами. Теория игр. Теория массового обслуживания. Имитационное моделирование.
Форма промежуточной аттестации:	Зачет

	Название:	**Безопасность в Интернет/Интранет**
	Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
	Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):	ПК-1, ПК-28, ПСК-8.4
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, криптокартаFortezza, 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:	Экзамен

Название:	**Защита абонентского телетрафика**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины	ПК-1, ПК-26, ПСК-8.4

(модуля):		
Результаты освоения дисциплины	**знать:**	сигналы электросвязи, принципы построения систем и средств связи
	уметь:	применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи;
	владеть навыками /иметь опыт:	навыками анализа основных характеристики возможностей телекоммуникационных систем по передаче информации
Содержание:		Теория телетрафика. Потоки вызовов. Телефонная нагрузка. Коммутация. Качество и дисциплина обслуживания вызовов. Методы анализа коммутационных систем. Распределение нагрузки и потерь в сетях связи. Схемы коммутации. Защита информации в телефонных каналах. Технологии защиты телефонных переговоров. Криптографическая защита телефонных сообщений. Основные понятия в области криптографической защиты телефонных сообщений. Криптографическое преобразование аналоговых телефонных сообщений.
Форма промежуточной аттестации:		Зачет

Название:		**Основы алгоритмизации**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-9, ПК-15, ПСК-8.4
Результаты освоения дисциплины (модуля)	**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 MicrosoftVisualStudio .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:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-9, ПК-15, ПСК-8.4
Результаты освоения дисциплины (модуля)	**знать:**	принципы представления, хранения и обработки информации с использованием компьютера; синтаксис и семантику как минимум одного императивного языка программирования; основные виды программного обеспечения современных ЭВМ для объектно-ориентированного анализа и проектирования синтаксис и семантику конструкций императивного языка программирования; простые структуры данных и методы с ними; состав и структуру стандартной библиотеки языка программирования
	уметь:	применять вычислительную технику для решения практических задач; применять принципы структурного и процедурного программирования для разработки программных продуктов; трассировать код простых функций; документировать код простых функций; формировать набор тестовых данных для тестирования функции реализовать динамические структуры данных в ОО-стиле; реализовать эффективные алгоритмы обработки данных; декомпозировать задачу на классы и модули; использовать стандартную библиотеку;
	владеть навыками /иметь опыт:	решения задач инженерной деятельности с помощью инструментальных средств информационных технологий применения инструментальной среды для разработки многомодульных программ; методами отладки и тестирования программ.
Содержание:		Принципы структурного и процедурного программирования для разработки программных продуктов; трассировка кода простых функций; документация кода простых функций; набор тестовых данных для тестирования функции. Динамические структуры данных в ОО-стиле. Эффективные алгоритмы обработки данных. Методы декомпозиции задачи на классы и модули; стандартную библиотеки.
Форма промежуточной аттестации:		Зачет с оценкой

Название:	**Криптографические протоколы**
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате	ПК-16, ПК-14, ПСК-8.4

освоения дисциплины (модуля):		
Результаты освоения дисциплины (модуля)	**знать:**	основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
	уметь:	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов
	владеть навыками /иметь опыт:	криптографической терминологией; навыками использования типовых криптографических алгоритмов;
Содержание:		Понятие криптографического протокола. Элементы протоколов. Основные протоколы. Промежуточные протоколы. Развитые протоколы. Эзотерические протоколы. Криптографические хэш-функции. Коды аутентификации. Схемы электронных подписей. Протоколы идентификации. Протоколы с нулевым разглашением. Протоколы передачи ключей. Протоколы распределения ключей. Управление ключами.
Форма промежуточной аттестации:		Зачет

Название:		**Защита сетевых протоколов**
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-14, ПК-18, ПСК-8.4
Результаты освоения дисциплины (модуля)	**знать:**	Модели взаимодействия открытых систем OSI, базовых топологий сетей, основных принципов обмена данными в локальных и глобальных сетях; Принципы построения локальных и глобальных сетей, назначение IP адресов; Протоколы обмена информацией в сетях, Протоколы информационной безопасности. протокола информационной безопасности электронной почты PGP, протокол сетевого уровня IPSec и др.
	уметь:	Настраивать сеть, определять параметры безопасного обмена данными в сети.
	владеть навыками /иметь опыт:	Разработки архитектуры сети, локализации трафика, определения текущего IP адреса, настройки DNS сервера; подключения компьютеров к сети, настройки и конфигурирования сети и сетевых устройств, поиска неисправностей, предоставления папок и сетевых устройств в общий доступ;
Содержание:		Архитектуры сети , основные сетевые протоколы. Классификация сетевых атак и способы их реализации. Методы борьбы с атаками. Защита протоколов прикладного уровня. Организация защиты информации на основе маршрутизаторов, межсетевых экранов, прокси-серверов. Построение VPN. Сетевые адаптеры
Форма промежуточной аттестации:		Зачет

Аннотации факультативных дисциплин

Название:		Инновационные технологии в сфере информационной безопасности
Название и номер направления и/или специальности:		10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля):		ПК-1
Результаты освоения дисциплины	**знать:**	современные направления инновационного развития в науке в сфере информационной безопасности
	уметь:	ориентироваться в современных направлениях, средствах и технологиях развития инновационного проектирования
	владеть навыками /иметь опыт:	навыками использования полученных знаний в различных областях науки, связанных с разработкой и применением новейших средств и технологий по информационной безопасности.
Содержание:		Проблемы вычисления на современных вычислительных машинах. Теоретически е пределы возможностей на современных ЭВМ Общие идеи работы квантовых компьютеров (КК). Возмущающие воздействия КК Сложностные классы. Общие идеи выполнения квантовых вычислений Классические и квантовые компьютеры: сравнение Линейные преобразования и их связь с квантовыми вычислениями Два подхода к решению проблем бесконечных данных при квантовых вычислениях. Точные реализации приближенных вычислений Проблема выбора базиса Схема выполнения квантовых вычислений: точность результата Основные идеи квантовой криптографии Передача информации в КК Общая процедура формирования квантового ключа шифрования. Квантовое распределения ключей Нанотехнологии. Понятие нанообъектов и их параметры. Физический предел изучения нанообъектов. Физические характеристики для выделении мезообъектов в качестве квантовых объектов Методы нахождения времени релаксации. Нанодатчики, (виды), сенсоры. Общая классификация. Использование нанотехнологий в сфере ИБ. Требования, предъявляемы к нанодатчикам. Мембранные сенсоры: структура, параметры, общее описание технологии изготовления. Тактильные сенсоры: основные характеристики, методы расчета. Бесконтактные оптические сенсоры. Струнные и сенсоры. Ядерно-магнитный резонанс. Ларморовская прецессия
Форма промежуточной аттестации:		Зачет

Название:	Технологии и средства обнаружения пропаганды экстремизма и терроризма в сети «Интернет»
Название и номер направления и/или специальности:	10.05.03 Информационная безопасность автоматизированных систем
Компетенции обучающегося, формируемые в результате освоения дисциплины	ПК-1, ПК-28, ПСК-8.4

(модуля):		
Результаты освоения дисциплины (модуля)	**знать:**	Психологических основы поведения участников экстремисткой деятельности. Идеалы и ценности разных народов, культур, религий. Технологии и средства обнаружения пропаганды экстремизма и терроризма в сети «Интернет», в том числе, социальных сетях. Средства маскирования такой деятельности. Психотип участников экстремисткой деятельности, людей, склонных к влиянию. Методы вовлечения в экстремисткие группы, технологии осуществления вербовки с применением информационных технологий и методов социальной инженерии. Меры противодействия экстремизму.
	уметь:	Уметь использовать методы толерантного взаимодействия в условиях социально дифференцированного общества, осуществлять оптимальный выбор поведения в условиях широкого распространения различных экстремистских идеологических течений. Уметь анализировать и выявлять признаки экстремисткой направленности у мододежи, у особых социальных групп, подверженных таким влияниям.
	владеть навыками /иметь опыт:	Владеть навыками анализа конкретных ситуаций, культурой диалога и восприятия альтернатив в ходе дискуссий по проблемам религиозно-политического экстремизма
Содержание:		Терроризм. Федеральный Закон №114-ФЗ "О противодействии экстремистской деятельности". Экстремистская деятельность (экстремизм), терроризм. основные причины экстремизма. Законодательство в этой сфере. Методы вовлечения в экстремистские группы, технологии осуществления вербовки с применением информационных технологий и методов социальной инженерии. Анонимность глобальной сети. Средства маскирования такой деятельности. Меры противодействия экстремизму. Контекстный анализ вербальных и невербальных средств информационного воздействия и содержательный аспект пользовательских страниц. Процессы выявления противоправного контента Интернет-пользователей и пользователей мобильных приложений. Взаимодействие с администрациями социальных сетей «Facebook», «Одноклассники», «Youtube» и другими. Краудсорсинг. Профилактика распространения радикальных идеологий в сети. Технологии и средства обнаружения пропаганды экстремизма и терроризма в сети «Интернет», в том числе, социальных сетях.
Форма промежуточной аттестации:		Зачет