УТВЕРЖДАЮ
Проректор по учебной работе
_____ Н.И. Архипова
«20» 03 2018 г.

Аннотации дисциплин образовательной программы по направлению
10.03.01 «Информационная безопасность»
(уровень бакалавриат)
Направленность (профиль):
«Комплексная защита объекта информатизации»

Блок 1	Дисциплины (модули)	Аннотации
Б1	**Базовая часть**	
1	ИСТОРИЯ. История России до XX века. История России XX века. История современной России.	Дисциплина «История» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрами: Истории России средневековья и нового времени, Истории России новейшего времени, УНЦ «Новая Россия. История постсоветской России». Целью курса является формирование целостного и исторически конкретного представления о российской цивилизации как сложной и динамичной системе, обладающей набором изменчивых характеристик и устойчивых доминант. Курс призван способствовать формированию у студентов целостного представления о прошлом России и её месте в системе мировых цивилизаций. Задачи: формирование комплексного представления об особенностях российского исторического процесса, о своеобразии развития и содержательных характеристиках социально-экономической, социально-политической и культурной жизни страны; овладение дисциплинарными основами исторического мышления и исследования; умение ориентироваться в современной гуманитарной литературе по предмету, научно аргументировать свою позицию по вопросам истории России, понимать взаимосвязь ключевых проблем развития России на современном этапе. Дисциплина направлена на формирование следующих компетенций: ОК-3 - способен анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма. В результате освоения дисциплины обучающийся

		должен: Знать: основные события и проблемы Отечественной истории. Уметь: на основе методологической культуры анализировать исторические события и факты, осуществлять познавательную деятельность, использовать гуманитарные знания в своей социальной и профессиональной деятельности. Владеть: основами исторических знаний как базы формирования научно-исторического мировоззрения, на основе которого формируется нравственный выбор, культура мышления, способность к обобщению, анализу, восприятию исторической информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме трех контрольных работ, промежуточная аттестация в форме трех зачетов. Общая трудоёмкость освоения дисциплины составляет 4 зачетные единицы.
2	ФИЗИЧЕСКАЯ КУЛЬТУРА	Дисциплина «Физическая культура» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой физического воспитания. Целью курса является формирование теоретических основ и практических навыков физической культуры личности и подготовка ее к профессиональной деятельности, а также создание необходимой теоретической базы для самостоятельных занятий спортом и физической культурой, формирование у студентов установок на здоровый образ жизни. Задачи: понимание роли физической культуры в развитии личности; формирование мотивационно-ценностного отношения к физической культуре, установки на здоровый образ жизни, физическое самосовершенствование, потребности в регулярных занятиях физическими упражнениями и спортом. Дисциплина направлена на формирование следующих компетенций: ОК-9 - способен использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: основные теоретические положения о медико-биологических характеристиках своего организма, врожденных физических качествах и способах их практического совершенствования; основные возрастные периоды развития физических качеств и особенности занятий физической культурой и спортом в эти периоды, иметь представления о современных видах физической культуры и спорта.

		Уметь самостоятельно составлять личную программу практических занятий по физической культуре. Владеть навыками грамотного построения и проведения самостоятельных занятий по физкультуре и осуществления контроля над своим физическим состоянием и развитием. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме проведения тестов физической подготовленности, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплин составляет 2 зачетные единицы.
3	ИНОСТРАННЫЙ ЯЗЫК. Части 1-4	Дисциплина «Иностранный язык» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой иностранных языков. Целью курса является обучение иностранному языку. Задачи: формирование и совершенствование у студентов навыков чтения, говорения, аудирования и письма. Дисциплина направлена на формирование следующих компетенций: ОК-7 - способен к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: значения лексических единиц, связанных с тематикой данного этапа обучения и соответствующими ситуациями общения, в том числе формами речевого этикета; значение изученных грамматических явлений. Уметь: вести диалог в рамках изученной тематики; рассказывать о себе, о своём окружении, своих планах; относительно полно и точно понимать высказывания собеседника в распространённых стандартных ситуациях повседневного общения; читать аутентичные тексты различных стилей (публицистические, художественные, научно-популярные, прагматические), используя основные виды чтения; писать личное письмо, заполнять анкету, письменно излагать сведения о себе в форме, принятой в стране/странах изучаемого языка, делать выписки из иноязычного текста; получать сведения из иноязычных источников информации (в том числе через Интернет), необходимых в целях образования и самообразования. Владеть: иностранным языком в объеме, позволяющем использовать зарубежную литературу по специальности; навыками разговорной речи на одном из иностранных языков и профессионально-ориентированного перевода текстов, относящихся к различным видам основной профессиональной деятельности. Рабочей программой предусмотрены следующие виды

		контроля: текущий контроль успеваемости в форме опроса, тестирования, аудиторной самостоятельной работы, доклада с презентацией, контрольной работы, ролевой игры, промежуточная аттестация в форме двух зачетов и двух экзаменов. Общая трудоемкость освоения дисциплины составляет 10 зачетных единиц.
4	СПЕЦИАЛЬНОЕ ДОКУМЕНТОВЕДЕНИЕ И ДОКУМЕНТАЦИОННОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ	Дисциплина «Специальное документоведение и документационное обеспечение управления» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование понимания закономерностей образования документов и способов их создания, развития систем документации и систем документирования, рассмотрение документа как объекта защиты и нападения, усвоение технологии эффективного поиска информации по профилю деятельности. Задачи: рассмотрение теоретических и прикладных аспектов документирования информации: свойств, функций и признаков документа, способов и средств документирования, структуры документа, порядка его составления и оформления, методов и способов защиты документа и документированной информации, классификации документов и систем документации, основ документационного обеспечения управления. Дисциплина направлена на формирование следующих компетенций: ПК-8 - способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-9 - способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: теоретические основы документоведения, его терминологию и задачи; свойства, функции и признаки документа; способы и средства документирования, классификацию типов носителей; нормативные требования к структуре документов, их составлению и оформлению; способы защиты документов от фальсификации; системы классификации документов; основы документационного обеспечения управления Уметь: руководствоваться нормативными документами по документоведению; составлять документы на любом носителе

		в зависимости от назначения, содержания и вида документа; применять способы и средства защиты документов и их носителей Владеть: навыками работы с документами; методами эффективного поиска документов по системам классификации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
5	ЭКОНОМИКА. Микроэкономка. Макроэконома.	Дисциплина «Экономика» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой теоретической и прикладной экономики. Целью курса является формирование представлений об основных принципах и тенденциях развития экономики. Задачи: изучение принципов и методов экономики; анализ основных теоретических положений экономики. Дисциплина направлена на формирование следующих компетенций: ОК-2 - способен использовать основы экономических знаний в различных сферах деятельности. В результате освоения дисциплины обучающийся должен: Знать: основные категории микро и макро экономики; цели и методы государственного экономического регулирования; методы и подходы, используемые в процессе анализа функционирования экономической системы, закономерности и принципы развития экономических процессов на микро и макро уровня; основы формирования и механизмы рыночных процессов на микроуровне; ценообразование в условиях рынка; формирование спроса и предложения на рынках производства; оценку эффективности различных рыночных структур; организационно-правовые формы предприятий; экономические ресурсы предприятия. Уметь: определять специфику ценообразования и производства в рыночных условиях; использовать приемы и методы для оценки экономической ситуации; оценивать экономические факторы развития предприятия. Владеть: навыками оценки деятельности предприятия с позиции внутреннего состояния и внешнего окружения, ориентируясь на кономические показатели. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме двух зачетов. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

6	ФИЛОСОФИЯ	Дисциплина «Философия» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой истории отечественной философии. Целью курса является целостное и систематическое освоение основных положений, проблем, идей, методов и способов понятийно-категориального, логико-семантического и стилистического выражения философского опыта - его истоков, начального становления. Задачи: привить студентам основные методы и навыки анализа оригинальных философских текстов, обеспечить усвоение студентами основных параметров развития важнейших школ и направлений философии. Дисциплина направлена на формирование следующих компетенций: ОК-1 - способен использовать основы философских знаний для формирования мировоззренческой позиции. В результате освоения дисциплины обучающийся должен: Знать: основную информацию о принципах философского мышления в различные исторические эпохи, а также содержание основных теорий различных философских школ. Уметь: работать с классическими философскими текстами. Владеть: навыками ставить вопросы, мыслить критично, самостоятельно, свободно. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
7	БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ	Дисциплина «Безопасность жизнедеятельности» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности группой гражданской обороны. Целью курса является формирование культуры общей безопасности, готовности и способности использовать приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности; характера мышления и ценностных ориентаций, при которых вопросы безопасности рассматриваются как приоритетные, особенно ярко выраженные при чрезвычайных ситуациях; их воздействии на человека и среду его обитания. Задачи: изучить характер чрезвычайных ситуаций и их последствия для жизнедеятельности; овладеть правовыми основами безопасности жизнедеятельности при возникновении

		чрезвычайных ситуаций; подготовить студентов к осознанным действиям в чрезвычайных ситуациях, научить грамотно применять способы защиты жизни и здоровья в сложившейся критической обстановке; сформировать навыки оказания первой помощи при ликвидации последствий аварий, катастроф, стихийных бедствий и эпидемиях. Дисциплина направлена на формирование следующих компетенций: ОПК-6 - способен применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности. В результате освоения дисциплины обучающийся должен: Знать: критерии безопасности технических систем; основные методы управления безопасностью жизнедеятельности; теоретические основы обеспечения безопасности; негативные воздействия чрезвычайных ситуаций на человека и среду обитания; основы защиты населения; основы оказания первой помощи населению; законодательные и правовые акты в области безопасности и охраны окружающей среды. Уметь: определять характер чрезвычайных ситуаций и их поражающие факторы; идентифицировать основные опасности среды обитания человека, оценивать риск их реализации; выбирать методы защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности; осуществлять мероприятия по защите; оказывать первую помощь при массовых поражениях населения и возможных последствиях аварий, катастроф, стихийных бедствий; принять нравственные обязанности по отношению к окружающей природе; понимать логику глобальных процессов в развитии основных характеристик среды безопасности и понимать их влияние на национальную безопасность России. Владеть: основными методами защиты персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий; понятийно-терминологическим аппаратом в области безопасности; методами обеспечения безопасности среды обитания и оказания первой помощи населению; путей снижения рисков безопасности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
8	ОСНОВЫ УПРАВЛЕНЧЕС-КОЙ ДЕЯТЕЛЬНОСТИ	Дисциплина «Основы управленческой деятельности» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность.

		Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование понимания методов и функций управленческой деятельности, умения осуществлять постановку управленческих задач, обосновывать принятие решений, определять ресурсы для их выполнения, давать оценку эффективности управления в различных условиях функционирования объекта. Задачи: рассмотрение основных понятий, связанных с управленческой деятельностью, концепций современных теорий управления, методов анализа управления, общей методики принятия управленческих решений. Дисциплина направлена на формирование следующих компетенций: ОК-6 - способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОК-8 - способен к самоорганизации и самообразованию; ПК-14 - способен организовывать работу малого коллектива исполнителей в профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: основные понятия и методы в области управленческой деятельности; природу управленческой деятельности и основные тенденции ее развития; особенности организации управленческой деятельности; закономерности управления различными системами; понятие, виды и признаки организации; составляющие внешней и внутренней среды организации; возможности использования информационных технологий в управленческой деятельности; основные функции управленческой деятельности; факторы эффективности управленческой деятельности. Уметь: оценивать эффективность управленческих решений; использовать зарубежный и отечественный опыт управления современными организациями; проводить оценку внешней и внутренней среды организации; планировать управленческую деятельность; использовать информационные технологии в управленческой деятельности; принимать эффективные решения, используя различные модели и методы принятия управленческих решений; оценивать эффективность управленческой деятельности; использовать внутреннюю и внешнюю мотивацию при управлении персоналом организации. Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения; анализа и оценки внешней и внутренней среды организации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3

		зачетные единицы.
9.1	ГУМАНИТАНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНСТИ. Социальные сервисы и сети.	Дисциплина «Гуманитарные аспекты информационной безопасности. Социальные сервисы и сети» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является подготовка к обеспечению информационной безопасности в социальной среде. Задачи: рассмотреть основные угрозы информационной безопасности в социальных сервисах и сетях, изучить методы и средства обеспечения информационной безопасности, изучить общие принципы, которые могут быть использованы для обеспечения организационно-правовой и технической защиты пользователей сети Интернет, концепции государственной политики в области защиты детей от информации, причиняющей вред их здоровью и развитию, рассмотреть способы организационно-правовой защиты от создания и распространения ненадлежащей рекламы и меры ответственности за нарушение российского рекламного законодательства. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: основные угрозы информационной безопасности в социальных сервисах и сетях; принципы и подходы, которые используются для обеспечения организационно-правовой и технической защиты пользователей сети Интернет; концепции государственной политики в области защиты граждан от информации, причиняющей вред их здоровью. Уметь: использовать нормативно-правовые документы в области защиты пользователей сети Интернет; применять правовые документы, касающиеся ответственности за нарушение российского рекламного законодательства. Владеть: навыками использования нормативных документов, регламентирующих информационную безопасность в социальных сервисах и сетях, навыками применения методов и средств обеспечения информационной

		безопасности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
9.2	ГУМАНИТАНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНСТИ. Информационное противоборство.	Дисциплина «Гуманитарные аспекты информационной безопасности. Информационное противоборство» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование понимания сущности, методов и способов реализации информационного противоборства, возможностей информационного воздействия на общество и личность. Задачи: формирование базовых теоретических понятий об информационном противоборстве как системы специальных мер обеспечения информационной безопасности объектов в условиях конкурентной борьбы в экономической и социальной сферах; создание представления об организации информационного противоборства в интересах обеспечения информационной безопасности личности, общества и государства; развитие способностей к управлению бизнесом в условиях конфликт ных интеллектуально-психологических противодействий со стороны конку рентов. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: место и роль информационных воздействий как факторов угроз национальной безопасности; характер и содержание угроз информационного воздействия на личность, общество, государство; роль информационного противоборства в обеспечении информационной безопасности Российской Федерации; основные международные правовые акты, регулирующие уровень интенсивности информационных воздействий и их снижение в интересах информационной

		безопасности личности, общества и государства; методы аналитической работы в интересах оценки информационной обстановки. Уметь анализировать и оценивать угрозы информационных воздействий на личность общество и государство; оценивать информационную обстановку и определять меры по нейтрализации угроз информационной безопасности; Владеть методикой организации информационного противоборства. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
10	МАТЕМАТИЧЕСКИЙ АНАЛИЗ. Части 1-2	Дисциплина «Математический анализ» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целью курса является обеспечить необходимую фундаментальную подготовку студентов к изучению и усвоению основных идей и методов современных разделов математики. Задачи: обеспечить овладение студентми современными методами исследования непрерывных процессов, используя понятийный аппарат дифференциального и интегрального исчисления и разработанные в анализе способы вычисления различных количественных характеристик. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач; В результате освоения дисциплины обучающийся должен: Знать: методы дифференциального и интегрального исчисления, ряды и их сходимость, разложение элементарных функций в ряд, методы решения дифференциальных уравнений первого и второго порядка. Уметь: исследовать функции, строить их графики, исследовать ряды на сходимость, решать дифференциальные уравнения, решать вычислительные задачи математического анализа на персональном компьютере. Владеть: аппаратом дифференциального и интегрального исчисления, навыками решения дифференциальных уравнений первого и второго порядка, навыками работы с библиотеками прикладных программ для решения задач математического

		анализа. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме двух экзаменов. Общая трудоемкость освоения дисциплины составляет 8 зачетных единиц.
11	ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧСКАЯ СТАТИСТИКА	Дисциплина «Теория вероятностей и математическая статистика» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целью курса является формирование базовых представлений о теории вероятностей и математической статистике под углом зрения их практического приложения в различных областях научных исследований и инженерной практики. Задачи: на примере комбинаторной теории вероятностей перейти к общим понятиям теории вероятностей и математической статистики, сформулировать основные теоремы, необходимые для понимания смежных дисциплин и практической деятельности. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач; ПК-11 - способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов. В результате освоения дисциплины обучающийся должен: Знать: случайные события и случайные величины, законы распределения; закон больших чисел, методы статистического анализа. Уметь: вычислять вероятности случайных событий, составлять и исследовать функции распределения случайных величин, определять числовые характеристики случайных величин; обрабатывать статистическую информацию для оценки значений параметров значимости гипотез. Владеть: вероятностным подходом к постановке и решению задач, навыками работы с библиотеками прикладных программ для решения вероятностных и статистических задач. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

12.1	АЛГЕБРА И ГЕОМЕТРИЯ. Линейная алгебра.	Дисциплина «Алгебра и геометрия. Линейная алгебра» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целью курса является подготовить выпускников, обладающих знаниями достижений классической математики, способных применять полученные знания в области информационной безопасности. Задачи: обеспечить уровень математической грамотности студентов, достаточный для формирования навыков математической постановки и решения классических оптимизационных задач и моделирования процессов; научить применять основные понятия и методы линейной алгебры для расчета различных количественных характеристик в задачах; сформировать навыки использования математических методов линейной алгебры при моделировании сложных процессов и принятии оптимальных управленческих решений. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: методы линейной алгебры; базовые понятия и основные технические приемы матричной алгебры и теории отображений линейных пространств. Уметь: использовать аппарат линейной алгебры; формулировать основные теоремы линейной алгебры; применять усвоенные алгебраические подходы для выработки оптимальных управленческих решений. Владеть: навыками решения задач линейной алгебры; навыками нахождения подходящего классического метода количественного анализа и моделирования. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
12.2	АЛГЕБРА И ГЕОМЕТРИЯ. Аналитическая геометрия.	Дисциплина «Алгебра и геометрия. Аналитическая геометрия» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целю курса является подготовка выпускников,

		обладающих знаниями достижений аналитической геометрии, способных применять полученные знания в области информационной безопасности. Задачи: формирование знаний и навыков исследования геометрических фигур и их свойств средствами элемаетарной алгебры, на основе метода координат. При этом методе каждому геометрическому соотношению ставится в соответстсвие некоторое уравнение, связывающее координаты фигуры. Дисциплина направлена на формирование следующих компетенций: - ОПК-2: способен применять соответствующий математический аппарат для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать методы аналитической геометрии; базовые понятия и основные технические приемы теории отображений линейных пространств. Уметь использовать аппарат аналитической геометрии; формулировать основные теоремы аналитической геометрии; применять усвоенные алгебраические подходы в решении прикладных задач. Владеть навыками решения задач аналитической геометрии для количественного анализа и моделирования. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
13	ДИСКРЕТНАЯ МАТЕМАТИКА	Дисциплина «Дискретная математика» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целью курса является формирование у студентов теоретических знаний и практических навыков по применению методов дискретной математики в процессе решения прикладных задач. Задачи: ознакомление с различными направлениями и методологией дискретной математики; обучение студентов теории и практике применения методов дискретной математики для поиска и обоснования решений в различных областях производства и управления. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных

		задач. В результате освоения дисциплины обучающийся должен: Знать: отношения эквивалентности и порядка, свойства операций над множествами, булевы функции и принцип двойственности, определения основных алгебраических структур, приемы построения СДНФ и СКНФ, элементарные тождества комбинаторики, детерминированные и ограниченно детерминированные функции, понятия: «граф», «деревья», «лес», детерминированные функции и деревья. Уметь: использовать свойства операций над множествами, построить СДНФ и СКНФ, строить таблицы истинности логических связок, строить многочлен Жигалкина для булевых функций, строить диаграмму Мура для функций, находить канонические уравнения для функций, определять вес дерева. Владеть: навыками топологической сортировки частично упорядоченного множества, выбора в указанном семействе подмножества наибольшего веса, построения СДНФ и СКНФ; проверки выводимости формулы G из множества формул S, построения диаграмм Мура, обхода графа в ширину и в глубину, симметричного обхода бинарного дерева. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
14	ТЕОРИЯ ИНФОРМАЦИИ	Дисциплина «Теория информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение навыков работы с понятиями теории информации и её использования в информационной безопасности. Задачи: формирование умения применять алгоритмы эффективного, помехозащищенного и криптографического кодирования; формирование понимания сути информационных процессов в системах передачи, хранения и преобразования данных. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: базовые понятия теории информации, свойства информации, подходы к измерению информации, свойства и меры информации, характеристики каналов связи, понятие и методы кодирования, алгоритмы кодирования.

		Уметь: осуществлять различные измерения информации, определять характеристики каналов связи, осуществлять кодирование информации. Владеть: алгоритмами кодирования информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
15	ФИЗИКА. Части 1-2	Дисциплина «Физика» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование естественно-научного мировоззрения, отвечающего современным требованиям научно-технического прогресса. Задачи: формирование понимания физической сущности и практической значимости электронных технических средств для обработки и защиты информации; получение практических навыков работы с лабораторными приборами измерений основных физических величин и экспериментального изучения процессов и явлений. Дисциплина направлена на формирование следующих компетенций: ОПК-1: способен анализировать физические явления и процессы для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: основные законы классической и современной физики, методы физического исследования; основные физические явления, процессы, основные физические поля и источники их излучения; единицы измерения физических величин; способы и лабораторные приборы измерения основных физических величин. Уметь: проводить экспериментальные научные исследования различных физических явлений и оценивать погрешностей измерения; выделять конкретную физическую сущность в прикладных задачах; применять полученные знания при освоении последующих инженерных дисциплин; обрабатывать результаты измерений и делать основные выводы; самостоятельно работать с учебной, научной и справочной литературой. Владеть навыками работы с современными техническими средствами для измерения физических величин. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме двух экзаменов.

		Общая трудоемкость освоения дисциплины составляет 7 зачетных единиц.
16	ЭЛЕКТРОТЕХНИКА	Дисциплина «Электротехника» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование понимания аналитических и машинных методов расчета электрических цепей, изучение физических явлений и эффектов, имеющихся в современной электронной аппаратуре и их учета при защите информации. Задачи: анализ вопросов, связанных с анализом и расчетом электрических цепей различной сложности, а также изучением современных методов расчета электрических цепей, основанных на компьютерных технологиях. Дисциплина направлена на формирование следующих компетенций: - ОПК-3: способен применять положения электротехники, электроники и схемотехники для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: основные элементы электрических сетейпостоянного и переменного тока с синусоидальными и импульсными источниками; общие понятия о процесссах протакающих (используемых) в современной электронной аппаратуре и их влияние на защиту информации; аналитические и машинных методы расчета электрических цепей; понятия о защите от поражающих факторов электрического тока. Уметь: осуществлять расчет электрических сетей с нелинейными и многополюсными элементами (диоды, транзисторы, операционные усилители), применяемыми в современной электронной аппаратуре; читать принципиальные схемы элетрических устройств; определять неисправность отдельных элементов в электрических цепях. Владеть: аналитическими и машинными методами расчета электрических цепей; навыками проверки элементов электриченских цепей; техникой безопасности при работе с электронной аппаратурой. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
17	ЭЛЕКТРОНИКА И СХЕМОТЕХНИКА	Дисциплина «Электроника и схемотехника» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность.

		Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является изучение принципов действия и особенностей применения типовых аналоговых и цифровых электронных устройств в современных технических средствах. Задачи: анализ вопросов, связанных с функционированием типовых аналоговых и цифровых электронных устройств. В лабораторном практикуме курса применяется компьютерная симуляция – программными средствами моделируется техническая задача и на этой основе отрабатываются различные варианты технических решений. Дисциплина направлена на формирование следующих компетенций: ОПК-3 - способен применять положения электротехники, электроники и схемотехники для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: общие понятия об устройстве и функционировании элементов электронных устройств и схемотехники. Уметь: читать принципиальные схемы элетронных устройств; определять неисправность отдельных элементов в типовых аналоговых и цифровых электронных устройствах; обслуживать электронных устройств в современных технических средствах. Владеть: навыками проверки элементов электронных устройств; техникой безопасности при работе с электронной аппаратурой. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
18	ИНФОРМАТИКА	Дисциплина «Информатика» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является ознакомление с основами информатики (терминами, базовыми понятиями и основными разделами), принципами функционирования современной вычислительной техники, достаточного для дальнейшего обучения профильным дисциплинам. Задачи: обучение основам информатики как научной фундаментальной и прикладной дисциплины; получение общего представления об устройстве и принципах функционирования вычислительной техники; формирование у студента достаточно полного и конкретного представления о

		специфике компьютерной информации, формах представления, способах передачи и методах обработки информации, принципах работы персональных компьютеров. Дисциплина направлена на формирование следующих компетенций: ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. В результате освоения дисциплины обучающийся должен: Знать: базовые понятия информатики, алгоритмизации; свойства информации, ее количественные характеристики; современные средства представления, обработки, хранения и распространения информации; основные этапы обработки данных на ЭВМ; основы алгоритмизации. Уметь: выбрать и конфигурировать компьютерную систему для решения комплекса задач в своей предметной области; использовать современные компьютерные технологии для создания и редактирования текстовой, числовой и визуальной информации; использовать информационные ресурсы Интернет для решения задач в своей профессиональной области. Владеть системным подходом в алгоритмизации решения прикладных задач. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
19	ТЕХНОЛОГИИ И МЕТОДЫ ПРОГРАММИРО-ВАНИЯ	Дисциплина «Технологии и методы программирования» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Целью курса является профессиональная подготовка студентов, необходимая для усвоения и глубокого понимания парадигм программирования и методов их реализации в программных продуктах. Задачи: приобретение базовых знаний в области разработки и проектирования программных продуктов; обучение студентов эффективной работе в современных интегрированных инструментальных средах; освоение типовых алгоритмов решения задач и современных подходов к построению программных средств. Дисциплина направлена на формирование следующих компетенций: ПК-2 - способен применять программные средства системного, прикладного и специального назначения,

		инструментальные средства, языки и системы программирования для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: парадигмы и методы создания программных продуктов, принципы, базовые концепции технологий программирования, основные этапы и принципы создания программного продукта; способы описания алгоритмов, основные принципы структурной и объектно-ориентированной мето-дологий программирования; особенности и возможности интегрированных сред разработки; синтаксис и семантику языков Free Pascal и Си. Уметь: формализовать исследуемую предметную область, используя необходимую алгоритмическую базу; создавать приложения с помощью инструментальных интегрированных сред; отлаживать и тестировать разрабатываемые программы, а также самостоятельно находить новые подходы для решения поставленных задач. Владеть основными приемами работы с современными инструментальными средствами, решать типовые и творческие задачи программирования. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
20	ЯЗЫКИ ПРОГРАММИРО-ВАНИЯ	Дисциплина «Языки программирования» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Целью курса является освоение современных инструментальных средств программирования посредством языка программирования Java. Задачи: изучение основных особенностей платформы и ее эволюции; углубление подходов объектно-ориентированного программирования; изучение методов создания эффективных алгоритмов и программ с использованием современных структур данных языка программирования Java, а также программной документации и способов оценки результатов работы программ. Дисциплина направлена на формирование следующих компетенций: ПК-2 - способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач. В результате освоения дисциплины обучающийся должен:

		Знать: основные концепции объектно-ориентированного программирования (инкапсуляция, наследования и полиморфизм), основные конструкции языка программирования Java, метолы программирования на языке высокого уровня Java, методы отладки программ и структуру программной документации. Уметь: ставить задачу, выбрать структуры данных и разработать эффективный алгоритм её решения; реализовать алгоритм средствами языка программирования Java; разрабатывать основную программную документацию. Владеть: методами проектирования эффективных алгоритмов обработки информационных структур и создания программной документации посредством Java. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
21.1	ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. Основная часть.	Дисциплина «Информационные технологии. Основная часть» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Целью курса является приобретение необходимых знаний в области современных компьютерных технологий и программных средств, умение ориентироваться в предложениях рынка современных программных продуктов. Задачи: познакомить студентов с современными технологиями сбора, хранения и обработки информации; дать представление о технологиях и программных средствах, используемых при разработке информационных систем; выработать навыки самостоятельных разработок информационных продуктов в среде современных программных средств и технологий, познакомить с основными средствами программирования разработки приложений и интерфейсов на стороне клиента и сервера; познакомить с NET. средой и основами NET-программирования; дать представление об основных моделях реализации в локальных сетях технологии «клиент- сервер», их достоинствах и недостатках; дать представление о ODBC – технологии, дать представление о сетевых технологиях Com, Corba, технических и программных средствах их реализации; интерфейсных программ и программ - приложений в среде СУБД Access, SQL Server; дать представление о языках XML, PHP, Java – Script, как о программных средствах для разработки Web – интерфейсов и Web – приложений. Дисциплина направлена на формирование следующих

		компетенций: ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты; В результате освоения дисциплины обучающийся должен: Знать: как используются современные информационные технологии для работы с информацией в профессиональной деятельности бакалавров; какие программные среды и технологии используются при разработке современных информационных систем; инструментальные средства современных СУБД; основы программирования в NET среде; основные технологии для работы с информацией в распределенных локальных сетях; технологии организации связей в многоуровневых локальных сетевых проектах; назначение и особенности компонентных - технологий, технические и программные средства их реализации; назначение и особенности технологий для распределенных информационных сетей, технические и программные средствах их реализации; программные средства для разработки Web – интерфейсов и Web - приложений в информационных проектах. Уметь: вести самостоятельные разработки в среде современных СУБД используя соответствующие информационные технологии; анализировать рынок программно-технических средств, информационных продуктов и услуг для решения прикладных задач и создания информационных систем; квалифицированно использовать инструментальные средства современных СУБД в информационных проектах; использовать инструментальные средства современных операционных систем, предназначенные для работы с информацией; использовать возможности процедурных расширений языка SQL и основные возможности ОО языков для разработки серверных программных объектов (триггеров, хранимых процедур, транзакций), программ-приложений, интерфейсных программ; использовать в информационных проектах основные возможности NET технологий; использовать в информационных проектах основные возможности языков XML, PHP, Java - Script для разработки Web – интерфейсов и Web – приложений; эксплуатировать и сопровождать информационные системы и

		сервисы. Владеть: навыками использования основных законов естественнонаучных дисциплин в профессиональной деятельности бакалавра; навыками обобщения, анализа, восприятия информации, постановки цели и выбора путей её достижения; навыками работы в коллективе, ответственности за поддержание партнерских, доверительных отношений; навыками использования современных информационных технологий в процессе создания, внедрения и эксплуатации информационных систем; навыками оценки качества программных продуктов, предлагаемых на информационном рынке; навыками эксплуатации и сопровождения информационных систем и сервисов; навыками работы с информацией в глобальных компьютерных сетях; навыками создания и управления ИС на всех этапах жизненного цикла. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме защиты лабораторных работ, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
21.2	ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. Операционные системы.	Дисциплина «Информационные технологии. Операционные системы» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Целью курса является формирование систематизированного представления о концепциях, принципах и моделях, положенных в основу построения операционных систем. Задачи: получение практической подготовки в области выбора и применения операционных систем для задач обработки информации, программирования в современных сетевых средах; изучение принципов функционирования операционных систем, связанных с обеспечением интерфейса прикладных процессов с аппаратными устройствами, многозадачности, ввода/вывода, управлением виртуальной памятью, процессами и потоками, реализации сервисов безопасности. Дисциплина направлена на формирование следующих компетенций: ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей

		функционирования объекта защиты; ПК-2 - способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты. В результате освоения дисциплины обучающийся должен: Знать: принципы построения, функционирования и внутренней архитектуры операционных систем (ОС), функциональность всех составных компонентов ОС и механизмы их взаимодействия в одно- и многопроцессорных системах, методы работы с внешними интерфейсами ОС, методы построения распределенных ОС, способы написания системных процедур, механизмы их функционирования в ОС, взаимодействии с системными функциями и инструментарием для их создания; основные характеристики и особенности современных операционных систем, сред и оболочек, методы и средства разработки и проектирования пользовательских приложений, особенности администрирования операционных систем в локальных и глобальных сетях. Уметь: использовать знания по архитектуре ОС для грамотной работы с ними, современные операционные системы и оболочки, и функциональные и сервисные программы; внутреннюю среду для написания программ, реализующие системные функции; применять офисные программные средства в повседневной работе; выбирать архитектуру персонального компьютера в соответствии с требованиями к условиям применения; устанавливать, эксплуатировать и администрировать операционные системы семейства Windows, Linux, использовать программные оболочки, командные интерпретаторы, навигаторы, проводники и файловые менеджеры. Владеть: навыками работы в различных операционных средах; навыками работы на персональном компьютере под управлением конкретной операционной системы и разработки приложений с использованием офисных программных средств; навыками работы с инструментальными средствами современных операционных систем, навыками решения прикладных задач в различных операционных средах. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме защиты лабораторных работ, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
22	АППАРАТНЫЕ СРЕДСТВА ВЫЧИСЛТЕЛЬНОЙ	Дисциплина «Аппаратные средства вычислительной техники» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность.

	ТЕХНИКИ	Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний и умений, необходимых для деятельности, связанной с эксплуатацией и обслуживанием современных средств вычислительной техники, а также подготовка обучаемых к грамотному и эффективному использованию компьютера как инструмента решения задач различной степени сложности в области информационной безопасности. Задачи: изучение арифметических и логических основ цифровых машин, элементов и узлов ЭВМ, принципов программного управления и микропроцессоров, периферийных устройств ЭВМ, архитектуры и принципов работы ПЭВМ, основ построения компьютерных сетей. Дисциплина направлена на формирование следующих компетенций: ПК-1 - способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: аппаратные средства вычислительной техники; принципы работы базовых элементов и устройств компьютеров; логические основы вычислительной техники и архитектуру основных типов современных аппаратных средств; структуру и принципы работы современных и перспективных микропроцессоров; состав и назначение функциональных компонентов компьютера. Уметь: выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; управлять компьютером, используя программирование на низком уровне; инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем. Владеть: профессиональной терминологией; методами решения задач управления и алгоритмизации процессов обработки информации; техническими программными средствами тестирования компьютеров с целью определения исправности компьютера и оценки его производительности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме защиты лабораторных работ, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
23	СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ	Дисциплина «Сети и системы передачи информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная

	ИНФОРМАЦИИ	безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является теоретическое изучение и практическое освоение принципов построения и функционирования современных сетей и систем передачи данных. Задачи: формирование знаний в области выбора, анализа и применения сетей и систем передачи данных; основных понятий и определений передачи информации, эталонной модели взаимодействия открытых систем (модель ISO/OSI, модель TCP/IP), архитектуры и средств взаимодействия процессов в сетях; рассматрение современных тенденций развития сетей связи. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. В результате освоения дисциплины обучающийся должен: Знать: основные принципы построения, архитектуру и топологию современных ЛВС, технологии Ethernet (FastEthernet, GigabitEthernet), TokenRing, FDDI – стандарты, принципы работы, сравнительные характеристики, преимущества и недостатки, основные средства построения современных ЛВС, классификации, внутреннюю архитектуру, режимы работы, протоколы сетевого уровня модели ISO/OSI; мультисервисные сети, технологии передачи голосового трафика VoIP, IP-телефонии. Уметь: анализировать и грамотно применять сети и системы передачи данных; реализовывать основные этапы построения сетей; иерархию моделей процессов в сетях; технологию управления обменом информации в сетях. Владеть: базовой терминологией по дисциплине, технологиями построения и сопровождения инфокоммуникационных систем исетей; навыками работы с инструментальными средствами тестирования и эксплуатации аппаратных и программных средств вычислительных устройств, комплексов, систем и сетей. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме защиты лабораторных работ, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
24	ОСНОВЫ ИНФОРМАЦИОННОЙ	Дисциплина «Основы информационной безопасности» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная

	БЕЗОПАСНОСТИ	безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний о совокупности задач в сфере науки, техники и технологий, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, понимания основных принципов, направлений и методов обеспечения информационной безопасности. Задачи: анализ вопросов, связанных с сущностью и значением информационной безопасности, её местом в системе национальной безопасности, определением теоретических, концептуальных, методологических и организационных основ обеспечения безопасности объектов информатизации, анализом методов и средств защиты информации. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. В результате освоения дисциплины обучающийся должен: Знать: основные понятия и базовые содержательные положения информационной безопасности и защиты информации; современную доктрину информационной безопасности; цели и принципы защиты информации. Уметь: выявлять факторы, влияющие на защиту информации; устанавливать структуры угроз защищаемой информации; раскрывать сущности компонентов и структуры систем защиты информации; ставить цели и выбирать пути эффективного решения задач в области информационной безопасности. Владеть: классификацией защищаемой информации по видам тайны; анализировать существующие угрозы информационной безопасности и пути их нейтрализации и устранения; подходами к созданию комплекса мер по защите информации предприятия; навыками подбора, изучения и обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме

		тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
25.1	ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Правовое обеспечение информационной безопасности.	Дисциплина «Правовое обеспечение информационной безопасности» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является приобретение знаний по основным положениям законодательства и нормативным правовым актам в области информационной безопасности, умения определять направления развития и совершенствования правового обеспечения в информационной сфере, а также формирование навыков использования законодательных и нормативно-методических документов, организационно-правовых мер и средств по обеспечению защиты информации. Задачи: изучение законодательной базы нормативного правового обеспечения информационной безопасности в России; информационной сферы как объекта правовых отношений, понятия тайны (государственной, коммерческой, служебной, профессиональной), как правового режима ограничения доступа к информации; рассмотреть особенности правового регулирования в сфере обращения с информацией о персональных данных; основные положения гражданского законодательства о правах на результаты интеллектуальной деятельности и средства индивидуализации; законодательства о техническом регулировании; правового регулирования лицензирования и норм сертификации средств защиты информации; ответственности за правонарушения в информационной сфере. Дисциплина направлена на формирование следующих компетенций: ОК-4 - способен использовать основы правовых знаний в различных сферах деятельности; ОПК-5 - способен использовать нормативные правовые акты в профессиональной деятельности; ПК-8 - способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-10 - способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по

		техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: место информационной безопасности в системе национальной безопасности; порядок защиты конституционного права граждан на информацию; основные виды информационнных правоотношений; основания возникновения и содержание правоотношений; принципы отнесения сведений к информации ограниченного распространения; основные положения, организационную структуру системы государственного лицензирования, знать особенности сертификации средств защиты информации по требованиям информационной безопасности; основные положения права интеллектуальной собственности; общие принципы юридической защиты за нарушения в области информационной безопасности. Уметь: определить место информационного права в системе российского права; применять источники права; применять способы защиты объектов интеллектуальных прав в общей системе информационной безопасности; применять нормы уголовного, административного законодательства для защиты интересов юридических и физических лиц. Владеть: навыками работы с государственной системой правового регулирования информационной безопасности; технологическим процессом защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
25.2	ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Организационное обеспечение информационной безопасности.	Дисциплина «Организационное обеспечение информационной безопасности» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является приобретение умения формировать системы организационной защиты информации, анализировать эффективность и разрабатывать направления развития таких систем; подготавливать нормативно-методические документы по регламентации организационного обеспечения информационной безопасности; организовывать охрану объектов и носителей; вести работу с персоналом, владеющим конфиденциальной информацией. Задачи: изучение сущности организационного обеспечения информационной безопасности в решении следующих задач:

		организацию работы по ограничению доступа к информации, лицензированию деятельности предприятий в области защиты информации, вопросам кадрового обеспечения и допуска граждан к государственной тайне, организационные аспекты деятельности персонала по защите информации, регламентацию системы доступа к защищаемой информации, организацию пропускного и внутриобъектового режимов, организационные требования к режимным помещениям, организацию совещаний (переговоров), издательской, рекламно-выставочной деятельности, проведение внутренних расследований по конфиденциальным вопросам. Дисциплина направлена на формирование следующих компетенций: ОПК-5 - способен использовать нормативные правовые акты в профессиональной деятельности; ПК-8 - способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-10 - способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: основные законодательные и нормативные акты в области информационной безопасности и защиты информации; принципы и методы организационной защиты информации; основы организации защиты государственной тайны и конфиденциальной информации; теоретические основы функционирования систем правового и организационного обеспечения информационной безопасности; цели, функции и особенности управления системами организационного обеспечения информационной безопасности в организациях; Уметь: применять основные положения законодательства в информационной сфере; разрабатывать направления совершенствования организационно-правовой защиты информации; анализировать эффективность систем организационного обеспечения информационной безопасности; - разрабатывать направления развития организационной защиты информации; пользоваться законодательными, нормативно-методическими документами по защите информации; разрабатывать нормативно-методические документы по регламентации систем организационной защиты информации. Владеть: навыками работы с законодательными, нормативно-методическими документами; методами формирования требований по защите информации; методами

		организации и управления деятельностью служб защиты информации на предприятии; методиками проверки защищенности объектов информатизации на соответствие требования нормативных документов; навыками организации и обеспечения режима секретности и конфиденциальности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
26	ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ	Дисциплина «Техническая защита информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является рассмотрение возникновения технических каналов утечки информации и возможности защиты информации техническими средствами. Задачи: освещение вопросов, связанных с анализом возможных технических каналов утечки информации и защиты объектов информатизации техническими способами и средствами, в том числе, проведением специальных исследований, обследований и специальных проверок. Дисциплина направлена на формирование следующих компетенций: ПК-3 - способен применять положения электротехники, электроники и схемотехники для решения профессиональных задач ПК-5 - способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; ПК-12 - способен принимать участие в проведении экспериментальных исследований системы защиты информации. В результате освоения дисциплины обучающийся должен: Знать: виды, формы и проявления угроз защищаемой информации, возникновение технических каналов утечки информации; методы и способы защиты информации техническими средствами; характер преднамеренного воздействия на информацию и способы его предотвращения. Уметь: осцществлять эффективную защиту объектов информатизации техническими способами и средствами, в том числе, с проведением специальных исследований,

		обследований и специальных проверок; формировать комплекс мер (правила, процедуры, практические приемы и пр.) для технической защиты информации на объекте информатизации. Владеть: навыками по подбору, установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации на объекте защиты. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
27	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний о базовых криптографических системах и схемах, их основных параметрах и умений применять на практике имеющиеся криптографические средства. Задачи: анализ общетеоретических вопросов криптографической защиты информации и практики применения ее методов и средств в современных информационных системах, синтеза и анализа криптографических протоколов, закономерностей построения сложных криптосистем, а также конкретных видов базовых криптографических протоколов и схем, получивших широкое применение в качестве инструментария для создания систем электронных платежей и систем документооборота в электронной коммерции. Дисциплина направлена на формирование следующих компетенций: ПК-1 -: способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; ПК-2 - способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: основы криптографической деятельности государства в условиях информационного противоборств; основные положения криптологии и практики криптографической защиты информации; нормативные правовые документы в области криптографической защиты информации; математические модели криптографических систем и

		криптографических протоколов; основные проектные решения, средства и методы криптографической защиты информации. Уметь: решать типовые задачи с помощью методов криптологии; аргументировано точно устанавливать параметры криптографических систем и криптографических протоколов; применять существующие криптографические системы и криптографических протоколы без снижения их стойкости за счет принятия неправильных эксплуатационных решений; шифровать/дешифровать информацию с помощью различных криптосистем (криптосистем с секретным и открытым ключами, гибридных криптосистем). Владеть: методами синтеза и анализа криптографических систем и протоколов, закономерностями построения сложных криптосистем; навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем документооборота в электронной коммерции. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
28.1	ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Основная часть.	Дисциплина «Программно-аппаратные средства защиты информации. Основная часть» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомление студентов с современными средствами защиты информации в компьютерных системах; овладение методами решения профессиональных задач; формирование навыков работы с современными программно-аппаратными средствами защиты информации; формирование понимания места указанных средств в системах передачи, хранения и преобразования данных. Задачи: идентификация/аутентификация средствами ОС; аппаратные модули доверенной загрузки; разграничение доступа средствами ОС; система защиты информации SecretNet; средства контроля защищенности распределенных систем. Дисциплина направлена на формирование следующих компетенций: ПК-1 - способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; ПК-2 - способен применять программные средства

		системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи данных; принципы организации информационных систем в соответствии с требованиями по защите информации. Уметь: формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности использованием различных программных и аппаратных средств защиты; пользоваться нормативными документами по защите информации; анализировать и оценивать угрозы информационной безопасности объекта. Владеть: методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; методами и средствами выявления угроз безопасности автоматизированным системам. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
28.2	ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Межсетевое экранирование, обнаружение вторжений.	Дисциплина «Программно-аппаратные средства защиты информации. Межсетевое экранирование, обнаружение вторжений» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомление студентов с основными понятиями в области межсетевого экранирования и систем обнаружения вторжения; осознание понимания места данных механизмов в общей архитектуре подсистемы защиты информации информационной системы; формирование навыков установки, настройки и реконфигурирования этих средств защиты информации; знакомство с нормативно-методической базой в части их применения. Задачи: изучение принципов фильтрации информационных потоков на границе сетей, идентификационных признаков потенциально опасных информационных потоков, сигнатур

		сетевых атак (вторжений), систем пакетной фильтрации, критериев фильтрации пакетов, управления информационными потоками посредством фильтрации, сопряжения и совместной эксплуатации систем межсетевого экранирования и систем обнаружения вторжений. Дисциплина направлена на формирование следующих компетенций: ПК-1 - способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; ПК-2 - способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: архитектуру и принципы функционирования межсетевых экранов и систем обнаружения вторжений, базовые функции и место в общей системе информационной безопасности; требования, предъявляемые к системам межсетевого экранирования и обнаружения вторжения отечественной нормативно-методической базой. Уметь: осуществлять установку и настройку типовых систем межсетевого экранирования и обнаружения вторжений как уровня узла, так и уровня сети, выполнять настройку систем пакетной фильтрации, встроенных в коммуникационное оборудование (на примере оборудования компании Cisco), выполнять выбор средств межсетевого экранирования, адекватных конфигурации защищаемой сети и имеющимся бизнес-процессам. Владеть: навыками оценки сетевого трафика с целью выделения потенциально опасных информационных потоков; определения признаков потенциально опасных потоков и формирования правил межсетевого экранирования, такие потоки исключающих. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
29	ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬ	Дисциплина «Основы управления информационной безопасностью» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных

	Ю	систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний по основам управления информационной безопасностью предприятия (организации) и методам повышения эффективности системы управления безопасностью объекта информатизации. Задачи: раскрыть требования международных и российских стандартов по информационной безопасности, классификацию систем управления, меры и средства управления информационной безопасностью, этапы внедрения систем управления. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-4 - способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: технологическое и организационное построение системы защиты информации; материально-техническое и нормативно-методическое обеспечение системы защиты информации; назначение, структуру и содержание управления системой защиты информации. Уметь: определять условия функционирования системы защиты информации; управлять системой защиты информации в условиях чрезвычайных ситуаций. Владеть: принципами и методами планирования, функционирования системы защиты информации; сущностью и содержанием контроля функционирования комплексной системы защиты информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
30.1	КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗА	Дисциплина «Комплексное обеспечение безопасности объекта информатизации. Организационное проектирование систем защиты информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность.

	ЦИИ Организационное проектирование систем защиты информации.	Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование представлений о теоретических и методологических основах организационного проектирования, порядка построения, оценки и совершенствования систем защиты информации предприятия (организации). Задачи: рассмотрение сущности и задач организационного проектирования систем защиты информации, методов исследования, принципов организации проектирования и этапов разработки проекта, технологию организации проектных работ. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-4 - способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-7 - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений; ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: методы, технологию и принципы проектирования систем защиты информации. Уметь: проводить предпроектное обследование, проводить анализ экономической целесообразности проектирования систем защиты информации; разрабатывать документы, необходимые для внедрения и функционирования системы защиты информации. Владеть: методикой определения структурного построения и состава системы защиты информации и разработкой организационно-нормативных документов, регламентирующих деятельность системы. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3

		зачетные единицы.
30.2	КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ Управление службой защиты информации.	Дисциплина «Комплексное обеспечение безопасности объекта информатизации. Управление службой защиты информации» является дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является создание у студентов представления о структуре службы защиты информации, принципах организации этой службы, о методах организации и управления службой защиты информации в качестве основного звена систем защиты информации. Задачи: рассмотрение места службы защиты информации в системе безопасности предприятия, описание функций службы защиты информации, описание методов определения оптимальной структуры и штатного состава службы защиты информации применительно к специфике ее функций, описание методов установление организационных основ и принципов деятельности службы защиты информации, описание методов подхода к общим и специфическим вопросам подбора и расстановки кадров, обучения, организации труда сотрудников службы защиты информации, анализ методов и технологии управления службой защиты информации. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-4 - способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; ПК-7 - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений; ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: о месте службы защиты информации в структуре организации, ее роли как ресурса организации и фактора производства; о правовых основах деятельности служб защиты

		информации на предприятиях; о хозяйственно-экономическом значении инвестиций в службу защиту информации; о методах оценки эффективности инвестиций в службу защиту информации. Уметь: анализировать состояние безопасности организации и правильно определять роль службы защиты информации в ее обеспечении; выбирать методы сопоставительного анализа эффективности инвестиционных проектов в службу защиты информации. Владеть: умением использовать нормативные правовые документы в своей профессиональной деятельности; способностью обоснования проектных решений по организации и управлению службой защиты информации; способностью собрать и провести анализ исходных данных для проектирования службы защиты информации; способностью разрабатывать предложения по совершенствованию системы управления службой защиты информации; методами изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности службы защиты информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
	Профильные дисциплины КЗОИ	
31.1	ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ И СИСТЕМЫ. Вычислительные сети.	Дисциплина «Информационные процессы и системы. Вычислительные сети» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Цель дисциплины: сформировать у студентов системные представления о принципах построения и использования телекоммуникационных средств и информационно-вычислительных сетей; ознакомить с основными архитектурными построениями локальных и глобальных информационных сетей; научить методам доступа к распределенным информационным ресурсам через соответствующие интерфейсы и практически ознакомить с системами поиска в информационныхсетях. Задачи: состоят в том, чтобы студенты имели представление о сетевых интерфейсах, сетевых программных и технических средствах, а также стандартизации и совместимости информационных сетей (ИС); понимали принципы построения и использования ИС; владели экономическими аспектами работы в сетях; имели опыт доступа к всемирным сетевым ресурсам. Дисциплина направлена на формирование следующих компетенций:

		ПСК-3.2 - способен формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты. В результате освоения дисциплины обучающийся должен: Знать: физические основы компьютерной техники и средств передачи информации, принципы работы аппаратных средств, принципы организации проектирования и содержание этапов процесса разработки программных комплексов; модели и структуры информационных сетей, информационные ресурсы сетей, теоретические основы современных информационных сетей. Уметь: формулировать требования к настраиваемым аппаратным и программным комплексам; реализовывать основные этапы построения сетей; иерархия моделей процессов в сетях, технологию управления обменом информации в сетях; поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества. Владеть: технологиями построения и сопровождения инфокоммуникационных систем и сетей; навыками работы с инструментальными средствами тестирования и эксплуатации аппаратных и программных средств вычислительных устройств, комплексов, систем и сетей. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
31.2	МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТОЕРИЯ АЛГОРИТМОВ	Дисциплина «Дискретная математика» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики. Целью курса является приобретение опыта применения логических понятий и символики, ознакомление с аксиоматическим методом и логическим выводом, с классическими вариантами построения общей теории алгоритмов, с алгоритмически разрешимыми и неразрешимыми проблемами. Задачи: рассмотрение вопросов исчисления высказываний, предикатов, вычислимости функций, решения диофантовых уравнений, решения задач комбинаторной оптимизации, а

		также рассмотрение проблематики решения NP-полных задач. Дисциплина направлена на формирование следующих компетенций: ПК-11 - способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; ПСК-3.1 - способен проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей. В результате освоения дисциплины обучающийся должен: Знать: основные понятия формальной логики, элементарной теории множеств (операции над множествами и основные факты, связанные с понятием мощности множества), (булевой) логики высказываний (включая вопросы полноты систем булевых функций), общей теории формальных исчислений и, более подробно, (классического) исчисления высказываний, а также (теоретико - множественной) логики предикатов и ее взаимоотношение с (формальным) исчислением предикатов. Уметь: применять математический аппарат при решении типовых задач, а также обнаруживать применимость аппарата математической логики для решения задач из родственных областей науки и ее приложений. Владеть: применять математический аппарат при решении типовых задач, а также обнаруживать применимость аппарата математической логики для решения задач из родственных областей науки и ее приложений. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
31.3	ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. Автоматизированные системы.	Дисциплина «Информационные технологии. Автоматизированные системы» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Целью курса является формирование у студентов знаний и умений построения автоматизированных информационных систем (АИС) и оценки их эффективности. Задачи: дать представление о составе и жизненном цикле АИС и этапах их проектирования; сформировать знания о типовых технических и программных средствах создания АИС; научить оценивать эффективность автоматизированных информационных систем; познакомить с тенденциями развития АИС. Дисциплина направлена на формирование следующих

		компетенций: ПСК-3.2 - способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты. В результате освоения дисциплины обучающийся должен: Знать: основные принципы и методы построения (формализации) и исследования математических моделей систем управления, классификацию, состав и особенности функционирования АИС; жизненный цикл АИС, его этапы; основы разработки и эксплуатации АИС; типовые технические, информационные, программные и другие средства АИС. Уметь: определять характеристики существующих автоматизированных информационных систем; проектировать АИС; оценивать эффективность АИС. Владеть: навыками определения характеристик существующих автоматизированных информационных систем; проектирования АИС; расчета эффективности АИС. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме защиты лабораторных работ, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
31.4	ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. Администрирование подсистем защиты информации	Дисциплина «Информационные технологии. Администрирование подсистем защиты информации» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомление студентов с методами формирования комплексной системы информационной безопасности; овладение методами проектирования и поддержки жизненного цикла систем информационной безопасности, формирование практических навыков по управлению и администрированию как отдельными компонентами, так и подсистемой защиты информации в целом, а также по разработке и внедрению предложений по оптимизации комплекса средств защиты информации. Задачи: рассмотрение базовых понятий в области жизненного цикла подсистемы защиты информации; элементы проектирования подсистемы защиты информации, разработка модели угроз и модели нарушителя, построение и последующая эксплуатация подсистемы защиты информации с учетом этих моделей; определения принципов администрирования подсистемы защиты информации, зоны ответственности и обязанностей администратратора

		информационной безопасности; формирование понимания сложности задачи интеграции подсистемы защиты информационной безопасности в информационную систему и администрирования ее без ущерба для целевой функции системы. Дисциплина направлена на формирование следующих компетенций: ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты; ПСК-3.2 - способностью формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты. В результате освоения дисциплины обучающийся должен: Знать: методологические и технологические принципы формирования и эксплуатации подсистемы защиты информации информационной системы; требования, предъявляемые к подсистеме защиты информации в нормативно-методической документации, методы и способы администрирования подсистемы защиты информации; методики оценки надежности ее функционирования. Уметь: участвовать в разработке моделей угроз и нарушителей, учитывать положения моделей при администрировании комплекса средств защиты информации; выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализированных наложенных. Владеть: навыками настройки и администрирования, а также модернизации комплекса средств защиты информации; управления сопряжением и совместной эксплуатацией разнородных средств защиты информации; документального сопровождения действий по эксплуатации и администрированию комплекса средств защиты информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
31.5	ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «Техническое регулирование в области защиты информации» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний по основным положениям законодательства и нормативным правовым актам в области защиты информации, принимаемым в рамках

		технического регулирования: национальных стандартов и стандартов организаций, других нормативных документов, а также по основным положениям обязательной сертификации продукции по требованиям безопасности информации. Задачи: рассмотреть особенности правового регулирования отношений в сфере обращения информации ограниченного распространения, правовые нормы сертификации средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ), вопросы ответственности за правонарушения в информационной сфере. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПСК-3.3 - способен участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты; ПСК-3.4 - способен организовать контроль защищенности и сопровождать аттестацию объекта информатизации в соответствии с нормативными документами. В результате освоения дисциплины обучающийся должен: Знать: нормативные правовые документы; нормативные и методические материалы по вопросам защиты информации и сертификации СЗИ и СКЗИ. Уметь: формировать комплекс организационных и нормативных мер (правил, процедур, практических приемов и др.) для проведения технического регулирования СЗИ и СКЗИ. Владеть: технологическим процессом проведения сертификации СЗИ и СКЗИ в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю Российской Федерации; Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
31.6	ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В АВТОМАТИЗИРОВАННЫХ	Дисциплина «Защита информационных процессов в автоматизированных системах» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных

	СИСТЕМАХ	систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности. Задачи: рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем; причин нарушения безопасности систем, существо проблемы обеспечения информационной безопасности, концептуальную модель безопасности, формирование требований к безопасности, основные механизмы обеспечения информационной безопасности систем; безопасный доступ к информационным ресурсам, формирование доверенных сред. Дисциплина направлена на формирование следующих компетенций: ПСК-3.1 - способен проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей; ПСК-3.3 - способен участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты. В результате освоения дисциплины обучающийся должен: Знать: методологические и технологические основы комплексного обеспечения безопасности АС; угрозы и методы нарушения безопасности АС; формальные модели, лежащие в основе систем защиты АС; стандарты по оценке защищенности АС и их теоретические основы; методы и средства реализации защищенных АС; методы и средства верификации и анализа надежности защищенных АС. Уметь: проводить анализ АС с точки зрения обеспечения компьютерной безопасности; разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы; применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС; реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС. Владеть: навыками работы с АС распределенных вычислений и обработки информации; навыками работы с документацией АС; приемами использования критериев оценки защищенности АС; приемами построения формальных моделей систем защиты информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов,

		контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
31.7	ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ	Дисциплина «Технические средства охраны» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование основных представлений о технических средствах охраны, охранно-пожарной сигнализации и видеонаблюдения, используемых на объектах информатизации. Задачи: освещение вопросов оборудования территории, зданий, помещений техническими средствами тревожной сигнализации и телевизионными системами видеонаблюдения, рассматриваются различные типы охранно-пожарных извещателей, построение и классификация систем охраны, принцип работы и технические характеристики извещателей, комплексирование систем охранной сигнализации и телевизионных систем видеонаблюдения. Дисциплина направлена на формирование следующих компетенций: ПСК-3.3 - способен участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты; ПСК-3.4 -: способен организовать контроль защищенности и сопровождать аттестацию объекта информатизации в соответствии с нормативными документами. В результате освоения дисциплины обучающийся должен: Знать: назначение и основные технические характеристики технических средств охраны и видеонаблюдения и ее место среди других направлений обеспечения информационной безопасности; квалификацию нарушителя, методы, способы и технические средства взлома, обхода технических средств охраны и видеонаблюдения (ТСО); методы, способы и технические решения по оборудованию и эксплуатации ТСО; показатели эффективности защиты и методы их оценки; основные руководящие, методические и нормативные документы по технической защите информации. Уметь: описывать (моделировать) объекты защиты; выявлять и оценивать источники угрозы, угрозы безопасности материальным и финансовым ресурсам, носителям конфиденциальной информации на конкретных объектах защиты; определять рациональные меры, методы и технические решения по охране объекта защиты, оценивать их эффективность; контролировать эффективность мер технической защиты информации.

		Владеть: навыками по выявлению возможных путей доступа на объект защиты и разрабатывать организационные и технические предложения по обеспечению безопасности объекта от физического доступа посторонних лиц. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
31.8	ПРОЕКТИРОВА-НИЕ СИСТЕМ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ	Дисциплина «Проектирование систем защиты объектов информатизации» является профильной дисциплиной базовой части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование представлений о теоретических и методологических основах организационного проектирования, порядка построения, оценки и совершенствования систем защиты информации предприятия (организации). Задачи: рассмотрение сущности и задач организационного проектирования систем защиты информации, методов исследования, принципов организации проектирования и этапов разработки проекта, технологию организации проектных работ. Дисциплина направлена на формирование следующих компетенций: ПК-7 - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений; ПСК-3.2 - способен формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты. В результате освоения дисциплины обучающийся должен: Знать: принципы, методы, технологию, основные этапы проектирования систем защиты информации. Уметь: проводить предпроектное обследование, проводить анализ экономической целесообразности проектирования систем защиты информации; разрабатывать документы, необходимые для внедрения и функционирования системы защиты информации. Владеть: методикой определения структурного построения и состава системы защиты информации и разработкой организационно-нормативных документов, регламентирующих деятельность системы.

		Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
Б1.В.ОД	**Вариативная часть**	
1	ФУНКЦИОНАЛЬНЫЙ ПРОЦЕСС И ОРГАНИЗАЦИЯ ПРЕДПРИЯТИЯ	Дисциплина «Функциональный процесс и организация предприятия» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование у студентов понимания, что эффективное функционирование современного предприятия и его оптимальная структура могут быть выбраны только по результатам анализа процессов, протекающих как внутри предприятия, так и при его взаимодействии с внешней средой. Задачи: формирование системы знаний по закономерностям развития предприятий различного типа и организации их функционирования с целью достижения максимальной эффективности при минимальных затратах; рассмотрение основных понятий и сущности предприятия, анализа среды, в которой функционирует предприятие, построение моделей функционирования предприятий; проведение структурного анализа предприятия, стратегии его развития, соотношение вертикальных и горизонтальных связей, общенаучные методы управления предприятиями, методы организационного проектирования и реорганизации предприятий. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. В результате освоения дисциплины обучающийся должен: Знать: об основных принципах формирования и функционирования различных предприятий; об основных понятиях и определениях в области теории и практики предприятий; о механизмах функционирования и принятия решений, организационных коммуникациях; о принципах управления предприятиями различных форм собственности и принципах их взаимодействия с государством, современных формах интеграции предприятий; о современной системе взглядов на управление предприятием; о методах анализа внешней и внутренней среды предприятия; об основных стратегиях развития предприятия, содержании основных

		стратегий конкуренции; о жизненном цикле продукта и стратегии создания нового продукта. Уметь: анализировать структуру предприятий в условиях централизованного и децентрализованного управления; определять стратегически наиболее эффективные в конкретной ситуации механизмы принятия решений, методы организации коммуникаций и межгруппового поведения; иметь практические навыки по анализу и формированию организационных структур, анализу эффективности организационных изменений. Владеть: навыками анализа структуры и функционирования предприятия, основными методами проектирования предприятий; навыками выработки механизмов принятия решений, направленных на обеспечение эффективного функционирования предприятия в высоко конкурентной среде. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольных опросов, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
2	СОЦИАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Дисциплина «Социальные аспекты информационной безопасности» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование культуры информационной безопасности в социальной среде. Задачи: изучить основные угрозы информационной безопасности в социальной среде, а также правовые и организационные принципы и методы обебеспечения информационной безопасности. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ОК-6 - способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОК-7 - способен к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности; ОК-8 - способен к самоорганизации и самообразованию. В результате освоения дисциплины обучающийся должен: Знать: социальные особенности формирования информационной безопасности различных групп населения;

		основные направления деятельности государственных органов и общественных организаций по формированию информационной безопасности; основные аспекты проблемы обеспечения информационной безопасности общества. Уметь: комплексно анализировать основные факты и явления влияющие на информационную безопасность социальных групп; анализировать информационную безопасность различных уровней: личности, общества, государства и т.д. Владеть: навыками культуры информационной безопасности; применять нормативные документы, регламентирующие информационную безопасность в обществе. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
3	МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «Математические основы защиты информации» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является развитие способностей к логическому и алгоритмическому мышлению; получение студентами знаний в сфере математических основ криптографии и защиты информации, необходимых для решения теоретико-практических задач. Задачи: изучение основ одноключевых криптосистем, классических приёмов и методов шифрования перестановкой, шифров замены, шифрования на основе маршрутов Гамильтона, обратимости и вычисления обратных величин, расширенного алгоритма Евклида, функции Эйлера и основ двухключевых (асимметричных) криптосистем, схемы шифрования RSA и атаки её методом факторизации, конечных полей Галуа, основных представлений об оценке сложности алгоритмов, схемы разделения секрета на основе древнекитайской теоремы об остатках. Дисциплина направлена на формирование следующих компетенций: ОПК-2 - способен применять соответствующий математический аппарат для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: математические основы и важнейшие механизмы криптографической защиты и смены её параметров; основные требования к криптографической защите информации. Уметь: определять, учитывать и анализировать качественные и количественные особенности составляющих

		криптографической защиты; формировать предложения, направленные на повышение криптостойкости. Владеть подходами к постановке и решению основополагающих теоретико-практических задач криптографического характера с применением необходимого математического аппарата. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
4	ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «Физические основы защиты информации» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомить студента с системой знаний, необходимой для формирования понимания роли и сущности физических явлений в образовании и противодействии утечке информации. Задачи: включают с себя вопросы, связанные с изучением физических явлений и законов, необходимых для понимания формирования технических каналов утечки информации; физических основы образования каналов утечки информации; физических полей различной природы, как носителей информации об объектах; физических основ акустических каналов утечки информации; физических основ оптических каналов утечки информации; физических основ радиоэлектронных каналов утечки информации; побочных радиоизлучений и наводок (ПЭМИН). Дисциплина направлена на формирование следующих компетенций: ПК-9 - способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; ОПК-1 - способен анализировать физические явления и процессы для решения профессиональных задач. В результате освоения дисциплины обучающийся должен: Знать: физические явления и законы, необходимые для понимания формирования технических каналов утечки информации; физические явления и законы, необходимые для обнаружения технических каналов утечки информации и их противодействию; методы и средства контроля утечки информации по техническим каналам; основные свойства физических полей, необходимые для освоения специальных дисциплин по защите информации; способы, средства и единицы измерения основных физических величин.

		Уметь: анализировать физические явления и законы, необходимые для обнаружения технических каналов утечки информации; выполнять работы со средствами контроля утечки информации по техническим каналам. Владет:ь навыками работы со средствами исследования физических явлений. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
5	БАЗЫ ДАННЫХ, СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ	Дисциплина «Базы данных, системы управления базами данных» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний и умений, необходимых для деятельности, связанной с созданием, управлением и использованием баз данных, а также подготовка обучаемых к грамотному и эффективному использованию баз данных для решения задач в области компьютерной безопасности. Задачи: освоение вопросов построения системы обработки баз данных, создание базы данных, моделирование базы данных, проектирование баз данных в рамках модели «сущность - связь», рассмотрение реляционной модели и нормализации, преобразование моделей «сущность - связь» в реляционные конструкции, реляционная алгебра, язык SQL, проектирование приложений баз данных, администрирование баз данных. Дисциплина направлена на формирование следующих компетенций: ПК-7 - способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений. В результате освоения дисциплины обучающийся должен: Знать: различные типы баз данных, способы моделирования баз данных, принципы проектирования баз данных, основы построения реляционных баз данных. Уметь: проектировать базы данных, создавать базы данных на основе проектов, эффективно управлять базами данных, инсталлировать, тестировать и использовать программные средства вычислительных и информационных систем, выбирать необходимые инструментальные средства для разработки, создания и управления базами данных; Владеть: профессиональной терминологией, методами решения задач управления процессами обработки

		информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
6	БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ	Дисциплина «Безопасность критически важных информационных систем» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение необходимого комплекса сведений по основным положениям безопасности критически важных информационных систем, формирование навыков проведения анализа и оценки рисков нарушения безопасности таких систем. Задачи: рассмотреть типовые модели критически важных информационных систем, модели нарушения безопасности, нормативную базу в области обеспечения безопасности, концептуальную модель безопасности, методы оценки рисков, особенности обеспечения безопасности программного обеспечения, обеспечение функциональной безопасности и надёжности, механизмы поддержания функциональной устойчивости, а также основные этапы организации безопасного функционирования критически важных информационных систем. Дисциплина направлена на формирование следующих компетенций: ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации. В результате освоения дисциплины обучающийся должен: Знать: классификацию автоматизированных систем управления критически важными объектами; категории критически важными объектами; модели возможных угроз и модели нарушителя информационной безопасности автоматизированной системы; методы и средства обеспечения безопасности критически важных информационных систем. Уметь: оценивать уровень информационной безопасности критически важной информационной системы; собирать и анализировать исходные данные для проектирования защищенных информационных технологий в автоматизированных системах сбора, обработки, хранения и передачи информации, вычислительных системах и

		компьютерных сетях; оценивать риски информационной безопасности автоматизированной системы. Владеть: профессиональной терминологией; методами оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих; методами решения задач управления и алгоритмизации процессов обработки информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
7	СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДСТУПОМ	Дисциплина «Системы контроля и управления доступом» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Содержание дисциплины охватывает круг вопросов, связанных с охраной объекта защиты от физического доступа посторонних лиц. Целью: является получение знаний по системам контроля и управления доступом, инженерно-техническим средствам охраны (СКУД и ИТСО) и формирование навыков работы по их использованию в системе защиты объекта от физического доступа посторонних лиц. Задачи по изучению дисциплины охватывают следующие вопросы: рассмотрение факторов, влияющих на защиту объекта от физического несанкционированного доступа; модель поведения нарушителя; определение категории объекта защиты; принципы и основные требования по обеспечению безопасности объекта защиты; разработка технических решений и порядка проведения работ по оборудованию объекта защиты СКУД и ИТСО. Дисциплина направлена на формирование следующих компетенций: ПК-3 -: способен администрировать подсистемы информационной безопасности объекта защиты; ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: назначение и основные технические характеристики СКУД и ИТСО, их взаимосвязь со средствами технической охраны и видеонаблюдения (ТСО и ВН); квалификацию нарушителя, методы, способы и технические средства взлома, обхода средств охраны объекта; методы, способы и

		технические решения по оборудованию и эксплуатации СКУД и ИТСО; показатели эффективности защиты и методы их оценки; основные руководящие, методические и нормативные документы по технической защите информации. Уметь: описывать (моделировать) объекты защиты; выявлять источники угроз, угрозы безопасности материальным и финансовым ресурсам, носителям информации, оценивать возможную величину ущерба от реализации угроз; определять рациональные меры, методы и технические решения применения СКУД и ИТСО по охране объекта защиты, оценивать их эффективность. Владеть: навыками по выявлению возможных путей физического доступа на объект защиты посторонних лиц, методикой по разработке законодательных, организационно-режимных и технических решений по обеспечению безопасности объекта защиты; правилами эксплуатации СКУД и ИТСО. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
8	БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ	Дисциплина «Безопасность операционных систем» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа. Задачи: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищенном исполнении. Дисциплина направлена на формирование следующих компетенций: ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты;

		ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа; нормативные правовые документы в области защиты информации; математические модели безопасности и формальные модели управления доступом в системах; модели и методы защиты операционных систем; основные проектные решения, средства и методы защиты информации от несанкционированного доступа. Уметь: решать типовые задачи с помощью методов и средств защиты информации от несанкционированного доступа; применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений; применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия; применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования. Владеть: методами разработки и использования защищенных программных средств; навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
9	СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА. Части 1-2.	Дисциплина «Системы электронного документооборота» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование представления об электронном документе как новой составляющей в правовых отношениях. Задачи: выявление основных особенностей «электронного документа», базовых принципов взаимодействия электронного и аналогового «миров». Дисциплина направлена на формирование следующих компетенций: ПК-13 - способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

		ПСК-3.3 - способен участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты. В результате освоения дисциплины обучающийся должен: Знать: законодательные и нормативные документы в области электронного документооборота; сущность и значение информации в развитии современного общества, понятия электронного документооборота; методы защиты информации и технологии обработки информации; виды и особенности рисков, порождаемых системами документооборота; методы использования средств защиты информации при построении систем документооборота; методы обеспечения юридической силы электронных данных. Уметь: оценивать используемые системы документооборота с точки зрения обеспечения защищенности обрабатываемой информации и юридической силы электронных данных; разработать комплекс мер по обеспечению информационной безопасности электронного документооборота и организовать его внедрение и последующее сопровождение. Владеть: основной терминологией, методами и основными алгоритмами реализации защищенного электронного документооборота; методами обеспечения юридической силы электронных данных. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме двух экзаменов. Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц.
10	МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «Моделирование процессов и систем защиты информации» является дисциплиной в вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний о предмете и технологии моделирования применительно к защите информации, классификации и анализе базовых моделей, методах оценки эффективности моделирования. Задачи: раскрывают общие вопросы теории моделирования, особенности систем защиты информации как объекта моделирования, технологии создания и характеристик аналитических, имитационных, структурно-функциональных моделей систем защиты информации, а также методы анализа эффективности таких моделей. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и

		возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-12 - способен принимать участие в проведении экспериментальных исследований системы защиты информации; ПСК-3.1 - способен проводить анализ функционального процесса объекта информатизации с целью выявления вероятных угроз информационной безопасности, определения их источников и целей; В результате освоения дисциплины обучающийся должен: Знать: определение места и роли моделирования процессов в системах защиты информации (СЗИ) при проектировании и внедрении систем защиты; теоретические основы моделирования процессов защиты информаци; классификацию моделей СЗИ; основные этапы моделирования; понятия и особенности аналитических и имитационных моделей; основные базовые модели СЗИ. Уметь: применять основные базовые модели СЗИ на различных этапах проектирования СЗИ; использовать основные принципы формального описания процессов защиты. Владеть: навыками структурно-функционального анализа СЗИ; методами анализа эффективности моделирования СЗИ. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена. Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.
11	АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ	Дисциплина «Аттестация объектов информатизации» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России. Задачи: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации, изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия. Дисциплина направлена на формирование следующих

		компетенций: ОПК-5 - способен использовать нормативные правовые акты в профессиональной деятельности; ПК-5 - способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; ПК-10 - способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: организацию аттестации объектов по требованиям безопасности информации; способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов; виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия; инструментальные средства и системы программирования для решения профессиональных задач. Уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; проводить предварительный технико-экономического анализ и обоснования проектных решений по обеспечению информационной безопасности; оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности. Владеть: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
12	АКТУАЛЬНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ	Дисциплина «Актуальные тенденции в области защиты информации» является дисциплиной вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01

	ЗАЩИТЫ ИНФОРМАЦИИ	Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомление студентов с современными тенденциями в области защиты информации, новейшими подходами к построению подсистем информационной безопасности и актуальными изменениями в нормативно-методической базе в этой сфере. Дисциплина направлена на формирование следующих компетенций: ПК-9: способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. Задачи: рассмотрение следующих актуальных тенденций в области защиты информации: интегрированные решения по защите информации; управление безопасностью информации и событий (SIEM-системы); управление учетными записями (IdAM-системы); унифицированный доступ к приложениям на примере Единой системы идентификации и аутентификации (ЕСИА); обеспечение безопасного взаимодействия с внешними информационными системами на примере Системы межведомственного электронного взаимодействия (СМЭВ); тенденции в применении средств криптографической защиты информации (средств легковесной криптографии), в том числе в системах электронного документооборота, использование «облачных» технологий при реализации механизмов безопасности; многоагентные системы в сфере информационной безопасности; безопасность Интернета вещей (Internet of Things, IoT). В результате освоения дисциплины обучающийся должен: Знать: перспективные направления развития информационной безопасности, наиболее актуальные решения в области криптографической, инженерно-технической и программно-аппаратной защиты информации, наиболее актуальные документы, создаваемые регуляторами в области информационной безопасности; особенности применения современных СЗИ для защиты персональных данных и информации, обрабатывающейся в государственных информационных системах. Уметь: ориентироваться на рынке современных средств защиты информации, выбирать оптимальное решение при проектировании и модернизации подсистемы информационной безопасности, выдвигать обоснованные предложения по применению таковых решений. Владеть: навыками интеграции и эксплуатации наиболее актуальных средств защиты информации, использования современных средств криптографической защиты информации и систем контроля и управления доступом. Рабочей программой предусмотрены следующие виды

		контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
13	КУРСОВАЯ РАБОТА ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ	Курсовая работа по защите информационных систем является вариативной частью блока Б1 учебного плана направления подготовки 10.03.01 Информационная безопасность. Курсовая работа реализуется кафедрой комплексной защиты информации. Целью курсовой работы является разработка технических предложений по защите информационных систем. Задачи: анализ информационной системы и угроз информационной безопасности, возникающих в ней; разработка технических предложений по защите информации в соответствии с требованиями нормативных документов отечественных регуляторов в области информационной безопасности. Курсовая работа направлена на формирование следующих компетенций: ПК-11 - способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; ПК-12 - способен принимать участие в проведении экспериментальных исследований системы защиты информации. В результате освоения дисциплины обучающийся должен: Знать: основные виды угроз безопасности для информационной системы; способы построения основных вариантов защиты от них. Уметь: проводить анализ проблем безопасности информационных систем с точки зрения обеспечения конфиденциальности и целостности данных; проводить анализ и обоснованный выбор средств защиты информации. Владеть: приемами настройки и применения современных средств защиты информации и средств криптографической защиты информации. Курсовая работа подлежит рецензированию научного руководителя и по результатам публичной защиты студенту выставляется оценка. Общая трудоемкость составляет 2 зачетные единицы.
14	КУРСОВАЯ РАБОТА ПО ПРОФИЛЮ ПОДГОТОВКИ	Курсовая работа по профилю подготовки является вариативной частью блока Б1 учебного плана направления подготовки 10.03.01 Информационная безопасность. Курсовая работа реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курсовой работы является закрепление и углубление теоретических и практических навыков полученных в процессе обучения по выбранному профилю. Задачи: проверка качества знаний, полученных студентом,

		его готовности к использованию теоретического материала для самостоятельного решения практических задач в области профессиональной деятельности; умения поставить цель и задачи исследования, методически правильно провести его, дать научно обоснованную оценку полученных результатов; продемонстрировать творческое использование профессиональных умений и навыков. Курсовая работа направлена на формирование следующих компетенций: ПК-10 - способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; ПК-11 - способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; ПК-12 - способен принимать участие в проведении экспериментальных исследований системы защиты информации. В результате выполнения курсовой работы обучающийся должен: Знать: методы сбора и анализа данных; методы обработки информации; возможности компьютерного анализа данных; возможности использования компьютерных сетей для получения данных; основные признаки текста; структуру и компоненты текста; принципы анализа текста; правила орфографии и редактирования. Уметь: классифицировать задачи и определять методы их решения, оценивать применимость метода для решения той или иной задачи; применять знания в учебной и профессиональной деятельности; использовать программное обеспечение; работать с информацией в глобальных сетях, читать тексты профессиональной направленности, целенаправленно отбирать, структурировать, анализировать научно-техническую и междисциплинарную информацию из научных источников; формулировать задачи в терминах статистических гипотез; участвовать в общественно-профессиональной дискуссии; использовать эти знания при решении специальных вопросов в области профессиональной направленности. Владеть: культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения; методами обработки информации; основными методами переработки данных; способами ориентации в профессиональных источниках информации; способностью оценивать информацию из источников и ее значимость; способностью интерпретировать и критически резюмировать полученную информацию из источников, навыками работы с программными средствами общего и профессионального назначения; методами и способами решения профессиональных задач в области информационной безопасности. Курсовая работа подлежит рецензированию научного руководителя и по результатам публичной защиты студенту

		выставляется оценка. Общая трудоемкость составляет 2 зачетные единицы.
Б1.В.ДВ	**Дисциплины по выбору по профилю КЗОИ**	
1.1	ОСНОВЫ ТЕОРИИ КОММУНИКАЦИИ	Дисциплина «Основы теории коммуникаций» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование коммуникативной профессиональной интеллектуальной установки, социально-культурная, теоретико-методологическая и практическая контекстуализация различных видов коммуникацации и связанных с ними практических вопросов. Задачи: рассмотрение феномена коммуникации в современном мире, социально-культурных и технологических предпосылок актуализации практик социальной коммуникаций; раскрытие содержания основных идей и понятий теории коммуникации в связи с российской национально-культурной традицией и потенциалом отечественного обществознания; обоснование методологических предпосылок исследования и изучения коммуникации в контексте современного научного познания; изучение содержания основных моделей коммуникации, учений и теорий ведущих мировых и отечественных исследователей коммуникации; характеристика прикладных теоретических аспектов в реализации основных видов коммуникации. Дисциплина направлена на формирование следующих компетенций: ОК-6 - способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОК-7 - способен к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: предпосылки становления феномена коммуникации в современном обществе и в российской социально-культурной среде; основные термины и понятия теории коммуникации; особенности основных видов коммуникации, возможности из изучения и практического использования; содержание основных направлений теоретического изучения коммуникации, соответствующие им методологические подходы и модели коммуникативного взаимодействия; факторы трансформации технологической среды коммуникации в современном мире, особенности различных средств и технологий коммуникации; прикладные аспекты

		теории коммуникации. Уметь: аргументировано характеризовать содержание основных направлений теоретического изучения и моделей коммуникации, в том числе с учетом их прикладных аспектов; осуществлять поиск информации в области теории коммуникации; выделять и практически учитывать в многообразии коммуникативных практик виды и базовые модели, а также используемые в коммуникативном взаимодействии средств и технологий. Владеть: приемами чтения и понимания основных теоретических текстов по коммуникативным наукам; методикой сбора информации по профилю деятельности; навыками письменной коммуникации в аннотировании, реферировании и прикладной аналитике теоретических текстов. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
1.2	РУССКИЙ ЯЗЫК И КУЛЬТУРА РЕЧИ	Дисциплина «Русский язык и культура речи» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой медиаречи. Целью курса является повышение уровня практического владения современным русским литературным и медийным языком. Задачи: в формировании у студентов основных информационных, исследовательских, когнитивных, креативных, коммуникативных, аксиологических и др. навыков, применительно к современному русскому литературному и медийному языку. Дисциплина направлена на формирование следующих компетенций: ОК-6 - способен работать в коллективе, толерантно воспринимая социальные, культурные и иные различия; ОК-7 - способнг к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: нормы современного русского языка в традиционной общелитературной и специальных областях; особенности формирования русского языка как социально-коммуникативной системы, имеющей многовековую историю развития; различные аспекты влияния факторов внешнего и внутреннего воздействия на складывающиеся представления о культуре речи.

		Уметь: осуществлять сравнительную характеристику языковых средств, используемых в разных сферах речевой деятельности; самостоятельно формировать представления о принципах составления текстов научной, публицистической и литературно-художественной направленности; проводить дискурсивный анализ различных типов текстов. Владеть: навыками установления определенной иерархии языковых единиц и принципами их функционирования в соответствии с современными представлениями о языковой норме и культуре речи; способами наиболее целесообразного использования языковых средств с учетом особенностей структуры и содержания текста; приемами стилистического комментария, описания и анализа текстов различных жанров. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
2.1	ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ	Дисциплина «История защиты информации» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является овладение знаниями о закономерностях становления и тенденциях развития и совершенствования системы защиты информации в России, соотношении (связи) процессов прошлого и событий современности; формирование способности критически применять и переосмысливать накопленный исторический опыт, перерабатывать большие объемы информации и проводить целенаправленный поиск в различных источниках информации по профилю деятельности. Задачи: изучение состава защищаемой информации на различных этапах развития государства; классификацию защищаемой информации в различные исторические периоды по видам тайны, собственнику и др.; структуру угроз защищаемой информации в различные исторические периоды; каналы несанкционированного доступа к защищаемой информации и методы ее добывания в различные исторические периоды; особенности государственной политики в области защиты информации; процесс развития и совершенствования нормативной базы защиты информации; состав органов защиты информации в различные периоды развития системы защиты информации; направления и методы защиты информации; факторы, определяющие современную систему защиты информации и тенденции ее развития; современные направления научных исследований в области истории защиты информации; проблемное поле и современное состояние исследований по историографии защиты

		информации. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. В результате освоения дисциплины обучающийся должен: Знать: особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды; основные направления государственной политики в области защиты; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты. Уметь: применять полученные знания в научно-исследовательской и практической работе; формулировать научные проблемы и иметь навык в поиске методов их решения; историографически обосновывать собственную исследовательскую проблему; применять навыки методологических операций в научно-исследовательской деятельности. Владеть: основными комплексами знания, которые включают в себя: понятия и термины, используемые и дискутируемые в различные исторические периоды становления и развития системы защиты информации, а также в современный период; основные исторические научные школы в области защиты информации и продукты их деятельности – научные концепции; главные труды крупнейших исследователей истории защиты информации. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
2.2	СИСТЕМЫ ЗАЩТЫ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ	Дисциплина «Системы защиты информации в зарубежных странах» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является овладение знаниями о закономерностях становления и тенденциях развития и

		совершенствования систем защиты информации в ведущих зарубежных странах, особенностях их современной организации и функционирования, перспективах развития и возможностях использования зарубежного опыта в России; формирование способности критически применять и переосмысливать накопленный зарубежный опыт, перерабатывать большие объемы информации и проводить целенаправленный поиск в различных источниках информации по профилю деятельности. Задачи: изучение в ведущих зарубежных странах процесса формирования и развития систем защиты информации; понятийного аппарата в области защиты информации; современного опыта организации систем защиты информации; правовых основ защиты информации; состава органов защиты информации; особенностей классификации защищаемой информации; особенностей и направлений международного сотрудничества в данной области. Дисциплина направлена на формирование следующих компетенций: ОК-5 - способен понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики; ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. В результате освоения дисциплины обучающийся должен: Знать: особенности процесса становления, развития и современной организации систем защиты информации в ведущих зарубежных странах; состав, особенности классификации, структуру угроз защищаемой информации в ведущих зарубежных странах; основные направления государственной политики в области защиты информации ведущих зарубежных странах; состав, структуру и основные направления деятельности органов защиты информации ведущих зарубежных; особенности нормативной базы защиты информации в ведущих зарубежных странах; международный опыт организации и совершенствования систем защиты информации. Уметь: применять полученные знания в научно-исследовательской и практической работе; формулировать научные проблемы и иметь навык в поиске методов их решения; использовать зарубежный опыт при разработке комплексной системы защиты информации. Владеть: основными комплексами знания: о тенденциях и перспективах развития систем защиты информации в ведущих зарубежных странах; об основных тенденциях и перспективах развития международного сотрудничества в области защиты информации.

		Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
3.1	ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ. Практикум.	Дисциплина «Экономика защиты информации. Практикум» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний об экономических методах защиты информации как части общих организационных мер, умении использовать современные методы расчетов для определения экономической целесообразности применения различных видов и средств защиты информации, обеспечивать выбор наиболее эффективных проектов инвестиций в защиту информации. Задачи: раскрывают вопросы, связанные с экономическими аспектами защиты информации, исследуются стоимостные показатели информации и виды ущерба, наносимые информации, даются основные подходы к определению затрат на защиту информации, оценка эффективности применяемых методов защиты и системы защиты информации в целом. Изучается вопросы управления ресурсами в процессе защиты информации, а также порядок формирования бюджета службы защиты информации на предприятии. Дисциплина направлена на формирование следующих компетенций: ПК-7- способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений. В результате освоения дисциплины обучающийся должен: Знать: основные экономические понятия и критери определения эффективности хозяйственно-экономической деятельности; о месте информации в структуре производства и ее роли как ресурса производства; об основах обеспечения экономической безопасности, методах ее обеспечения; об основных положениях определения экономической эффективности защиты информации; о методах оценки эффективности инвестиций в защиту информации; о содержании, видах и функциях страхования информации. Уметь: анализировать состояние экономической безопасности организации и правильно определять роль защиты информации в ее обеспечении; выбирать методы определения ущерба, наносимого обладателю информации в результате противоправного ее использования; определять расчетным и экспертным методами стоимостные оценки ущерба; анализировать информацию, возникающую в

		процессе производственно-хозяйственной деятельности, и вырабатывать рекомендации об экономической целесообразности ее защиты; выбирать методы сопоставительного анализа эффективности инвестиционных проектов по защите информации. Владеть: нормативно-правовыми документами по экономической составляющей систем защиты информации; способностью осуществлять технико-экономическое сопровождение и обоснование проектных решений по обеспечению информационной безопасности; способностью анализировать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
3.2	ОСНОВЫ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА	Дисциплина «Основы конфиденциального делопроизводства» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний по научным, прикладным и методическим аспектам организации работы конфиденциального делопроизводства. Задачи: изучение выполнения технологических стадий, процедур и операций с конфиденциальными документами, проектирование рациональной технологической схемы защищенного документооборота. Дисциплина направлена на формирование следующих компетенций: ПК-8 - способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов; ПК-9 - способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности. В результате освоения дисциплины обучающийся должен: Знать: необходимую терминологию; проблемы построения и совершенствования технологии защищенного документооборота. Уметь: применять разнообразные типы носителей документной информации (бумажные, электронные и др.). Владеть: различными средствами, способами и системами

		обработки и хранения конфиденциальных документов; навыками профессионального подхода к работе с конфиденциальными документами и построения защищенного документооборота. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
4.1	ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ	Дисциплина «Защиты персональных данных» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Целью курса является формирование знаний и умений для организации комплекса мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности персональных данных и используемых информационных технологий, способы снижения рисков утечки персональных данных. Задачи: сформировать знания базовых теоретических понятий, лежащих в основе обеспечения конфиденциальности обработки персональных данных; овладеть комплексом мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер; проводить классификацию информационных систем, создавать модели угроз, описывать систему защиты персональных данных. Дисциплина направлена на формирование следующих компетенций: ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: виды, источники и носители защищаемой информации; основные угрозы безопасности персональных данных; основные принципы и методы защиты персональных данных; основные руководящие и нормативные документы по технической защите персональных данных; порядок организации защиты персональных данных. Уметь: анализировать основные рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных

		данных; разрабатывать нормативно-методические документы по регламентации защиты персональных данных; организовывать работу по ведению делопроизводства, в области защиты персональных данных и формулирование основных технические требования обеспечения защиты персональных данных на локальном уровне. Владеть: навыками по классификации информационных систем; методами по определению актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; методиками по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
4.2	НЕЙРОННЫЕ СИСТЕМЫ	Дисциплина «Нейронные системы» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационных технологий и систем. Цель дисциплины: изучение основных принципов организации информационных процессов в нейрокомпьютерных системах. Задачи: изучение областей применения нейронных сетей: распознавание образов, принятие решений, кластеризация, прогнозирование, аппроксимация, сжатие данных; изучение методики синтеза нейронных сетей различной структуры; исследование надежности и диагностики нейронных сетей;изучение принципов построения нейрокомпьютеров; формирование навыков разработки и реализации программных моделей нейронных сетей и нейрокомпьютерных систем. Дисциплина направлена на формирование следующих компетенций: ПК-12: способен принимать участие в проведении экспериментальных исследований системы защиты информации. В результате освоения дисциплины обучающийся должен: Знать: основные принципы организации информационных процессов в нейрокомпьютерных системах; основные архитектуры нейронных сетей, нейрокомпьютерных систем и области их применения; основные способы и правила обучения нейрокомпьютерных систем. Уметь: анализировать и описывать нейроструктуры; делать оценки и сравнивать качество обучения и функционирования различных моделей нейрокомпьютерных систем.

		Владеть: навыками анализа и описания нейроструктур; навыками разработки и реализации программных моделей нейрокомпьютерных систем. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
5.1	УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ	Дисциплина «Управление информационными системами» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности. Цель дисциплины: формирование у студентов понимания сущности управления действующими информационными системами, формирование у студентов системы знаний о принципах, методах управления действующими ИС, а также системы навыков моделирования и проектирования бизнес процессов управления ИТ-услугами. Задачи: сформировать научный подход к формированию и реализации процессов управления современными информационными системами; научить студентов современным методам и технологиями процессного подхода к управлению современными информационными системами и их сервисами; научить практическим приемам эффективной организации поддержки и предоставления ИТ-услуг всем подразделениям предприятия или организации, создавая тем самым условия для обеспечения совместной их деятельности и реализации непрерывного и безопасногобизнеса. Дисциплина направлена на формирование следующих компетенций: ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: об основных методологиях и технологиях управления информационными системами; основные понятия жизненного цикла информационной системы, его стадии, процессы и модели жизненного цикла ИС; теоретические и организационно-методические основы организации и управления проектами информационных систем и управления

		информационными услугами; состав процессов управления информационными системами; Уметь: использовать методы и программные средства структурного, стоимостного и динамического анализа информационными системами и формирования решений на их основе по реорганизации и процессному управлению; проводить реализацию проектных решений с использованием современных информационно-коммуникационных технологий и технологий программирования; участвовать в управлении проектами информатизации предприятий и организаций; проводить работы по сопровождению и эксплуатации ИС. Владеть работы в коллективе в процессе управления информационными системами и их сервисами; анализа и оценки экономических затрат на функционирование информационных систем; работы с современными программными продуктами, используемыми в процессе управления информационными системами, в частности системой MS Project Expert. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
5.2	БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	Дисциплина «Безопасность программного обеспечения» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний о базовых методах и способах защиты ПО автоматизированных систем и умений применять на практике средства защиты программ, имеющиеся на отечественном рынке продукции и услуг в области защиты информации от несанкционированного доступа. Задачи: рассмотрение следующих вопросов: основные понятия теории алгоритмов и теории сложности вычислений; методы анализа ПО; методы защиты разрабатываемых программ от автоматической генерации инструментальными средствами программных средств скрытого воздействия; методы идентификации программ и их характеристик; методы защиты программ от компьютерных вирусов; методы защиты программ от исследования; методы обфускации программ; методы защиты программ от несанкционированного копирования; средства и системы тестирования программного обеспечения при испытаниях его на безопасность; операционные системы в защищенном исполнении. Дисциплина направлена на формирование следующих компетенций: ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с

		нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа; нормативные правовые документы в области защиты информации; математические модели безопасности и формальные модели управления доступом в системах; модели и методы защиты операционных систем; основные проектные решения, средства и методы защиты информации от несанкционированного доступа. Уметь: решать типовые задачи с помощью методов и средств защиты информации от несанкционированного доступа; применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости за счет принятия неправильных эксплуатационных решений; применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия; применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования. Владеть: методами разработки и использования защищенных программных средств; навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опросов, промежуточная аттестация в форме зачета с оценкой. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
6.1	ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ, УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ	Дисциплина «Инфраструктура открытых ключей, удостоверяющие центры» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является приобретение знаний о базовых криптографических схемах с открытым ключом, их основных параметрах и умений применять на практике криптографические средства, имеющиеся на отечественном рынке продукции и услуг в области криптографической защиты информации. Задачи: изучение следующих основных вопросов: основные понятия криптологии; теоретико-сложностные аспекты криптографических схем с открытым ключом, в том числе схем электронной подписи; основные положения Федерального закона «Об электронной подписи» и ГОСТ Р 34.10-2012; инфраструктура открытых ключей; принципы

		использования, виды и средства электронной подписи; удостоверяющие центры; сертификаты ключей проверки электронной подписи, поля сертификата ключа проверки электронной подписи. Дисциплина направлена на формирование следующих компетенций: ПК-1 - способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. В результате освоения дисциплины обучающийся должен: Знать: основные положения криптологии и практики криптографической защиты информации; математические модели криптографических схем с открытым ключом; основные средства и методы криптографической защиты информации. Уметь: решать типовые задачи с помощью методов криптологии; аргументировано точно устанавливать параметры криптографических схем с открытым ключом; применять инфраструктуру открытых ключей (PKI-инфраструктуру); работать с сертификатами открытых ключей (ключей проверки подписи. Владеть: методами синтеза и анализа криптографических схем с открытым ключом; навыками эксплуатации криптографических схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем электронного документооборота. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
6.2	ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	Дисциплина «Защита информации от несанкционированного доступа» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от несанкционированного доступа (НСД); формирование навыков, необходимых для защиты информации от НСД в современных информационных системах. Задачи: овладение методами решения профессиональных задач по защите информации от НСД; формирование навыков работы с современными средствами защиты информации от НСД. Дисциплина направлена на формирование следующих

		компетенций: ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. В результате освоения дисциплины обучающийся должен: Знать: основные модели доступа (мандатная, дискреционная, ролевая и др.), принципы и методы защиты информации от НСД; принципы организации информационных систем в соответствии с требованиями по защите информации от НСД. Уметь: формулировать и настраивать политику безопасности в информационной системе; осуществлять меры по защите информации от НСД, пользоваться нормативными документами по защите информации от НСД; анализировать и оценивать угрозы безопасности информационной системы. Владеть: методикой анализа защищенности информационной системы; методами и средствами выявления угроз ее информационной безопасности. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
7.1	БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ НА БАЗЕ TCP/IP	Дисциплина «Безопасность информационных технологий и сетей на базе TCP/IP» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является обучение студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей на базе TCP/IP. Задачи: анализ следующих основных вопросов: технологии обеспечения безопасности в сетях на базе TCP/IP; угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем; типовые модели атак, направленные на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения; возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях; принципы функционирования основных защищенных сетевых протоколов; основы приме-нения межсетевых экранов; определение политики сетевой безопасности; методы

		и средства проектирования, реализации и оценки защищенных сетевых систем. Дисциплина направлена на формирование следующих компетенций: ПК-3 - способен администрировать подсистемы информационной безопасности объекта защиты; ПК-6 - способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации; ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. В результате освоения дисциплины обучающийся должен: Знать: принципы построения и функционирования, примеры реализаций компьютерных сетей на базе стека протоколов TCP/IP; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях. Уметь: эффективно использовать различные методы и средства защиты информации для компьютерных сетей на базе стека протоколов TCP/IP; администрировать компьютерные сети; проводить мониторинг угроз безопасности сетей. Владеть: навыками эксплуатации и администрирования компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
7.2	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ	Дисциплина «Информационная безопасность мобильных устройств» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является ознакомить слушателя с типовой системой безопасности мобильных устройств и привить навыки безопасной их настройки. Задачи: включают в себя рассмотрение вопросов, связанных с архитектурой мобильных устройств, современными операционными системами управления мобильными устройствами, механизмами безопасности, присутствующими в этих решениях, и типовыми угрозами и сценариями атак на

		мобильные устройства. В качестве операционных систем, под управлением которых работают мобильные устройства, рассматриваются современные версии ОС Microsoft, iOS и Android. Определяются средства аутентификации субъектов доступа и авторизации доступа, ограничения программной среды и проверки устанавливаемых программных модулей. Рассматриваются типовые угрозы, такие как спуфинг, фишинг и т.д. Предлагаются подходы к безопасному внедрению концепции BYOD. Дисциплина направлена на формирование следующих компетенций: ОПК-4 - способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ПСК-3.3 - способен участвовать в реализации комплекса организационно-технических мер по обеспечению информационной безопасности объекта информатизации, осуществлять установку, настройку и обслуживание элементов защиты. В результате освоения дисциплины обучающийся должен: Знать: основные понятия информационной безопасности в предметной области; архитектуру мобильных устройств; основные угрозы безопасности мобильных устройств. Уметь: администрировать подсистемы информационной безопасности объекта; использовать инструментальные средства и системы программирования для решения профессиональных задач. Владеть: базовыми механизмами обеспечения информационной безопасности мобильных устройств. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.
8.1	СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (DLP-СИСТЕМЫ)	Дисциплина «Системы защиты от утечки конфиденциальной информации (DLP-системы)» является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является обучение студентов основам построения и эксплуатации DLP-систем (Data Leakage Protection System), принципам и методам защиты информации

		от утечки в корпоративных информационных системах за счет обнаружения и блокирования несанкционированной сетевой передачи информации со стороны пользователей, которые имеют право доступа к конфиденциальным данным. Задачи: классификация DLP-систем по способу обнаружения утечки данных, по способу распознавания критичных документов (по ключевым словам или выражениям, по заранее созданным цифровым «отпечаткам» конфиденциальных документов и др.); анализ угроз информационной безопасности, устраняемых DLP-системами и требований, предъявляемые к ним, принципы работы DLP-систем, исследование и анализ отечественного рынка DLP-систем, в том числе сертифицированных. Дисциплина направлена на формирование следующих компетенций: ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; ПК-15 - способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации; ОПК-7 - способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. В результате освоения дисциплины обучающийся должен: Знать: угрозы нарушения информационной безопасности в корпоративной информационной системе, методы предотвращения утечки конфиденциальной информации; методы и средства построения DLP-систем. Уметь: проводить анализ корпоративных информационных систем с точки зрения обеспечения их информационной безопасности; разрабатывать модели и политику безопасности для них; реализовывать DLP-системы в соответствии со стандартами по оценке защищенности АС. Владеть: навыками работы с DLP-системами в рамках корпоративной информационной системы; приемами их использования для предотвращения утечки критичных корпоративных данных. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.
8.2	ОРГАНИЗАЦИЯ	Дисциплина «Организация виртуальных частных сетей»

	ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ	является дисциплиной по выбору вариативной части блока Б1 учебного плана по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на факультете информационных систем и безопасности кафедрой комплексной защиты информации. Целью курса является формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по применению виртуальных частных сетей, оптимального выбора и интеграции сетевых протоколов виртуальных частных сетей (ВЧС). Задачи: рассмотрение существа проблемы безопасной передачи информации в информационных системах, основных способов обеспечения конфиденциальности и целостности информации при её передаче, основных протоколов, применяемых для организации защищенных ВЧС, критериев выбора оптимальных схемных решений для организации защищенных ВЧС на канальном, сетевом и прикладном уровнях. Дисциплина направлена на формирование следующих компетенций: ПК-13 - способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации. В результате освоения дисциплины обучающийся должен: Знать: основные виды угроз безопасности информации при ее передаче по компьютерным сетям; способы построения виртуальных каналов; протоколы организации ВЧС. Уметь: проводить анализ проблем безопасности передачи информации с точки зрения конфиденциальности и целостности; проводить анализ и выбор сетевых протоколов ВЧС. Владеть приемами настройки и применения современных сетевых протоколов ВЧС. Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме лабораторных работ, промежуточная аттестация в форме зачета. Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы.