

**Аннотация рабочих программ дисциплин в соответствии с учебным  
планом подготовки бакалавров по направлению подготовки 10.03.01  
Информационная безопасность**

**ГУМАНИТАРНЫЙ, СОЦИАЛЬНЫЙ И ЭКОНОМИЧЕСКИЙ ЦИКЛ  
(БАЗОВАЯ ЧАСТЬ)**

**Б1.Б.1. «Философия»**

Дисциплина «Философия» относится к базовой части гуманитарного, социального и экономического цикла основной образовательной программы по специальности 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее полученных знаниях по дисциплинам «История», «Правоведение», «Экономика», «Концепции современного естествознания».

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма;

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

Содержание дисциплины включает в себя круг философских проблем и методов их исследования, в том числе связанных с будущей профессией; основные разделы философского знания; философия, ее предмет и значение, исторические типы философии, онтология, гносеология, философия и методология науки, социальная философия, философия истории, философская антропология.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 час. Преподавание дисциплины ведется на 2-ом курсе в 3 семестре продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 3 семестре.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин, прохождения практики, итоговой государственной аттестации и выполнения выпускной квалификационной работы бакалавра.

### **Б1.Б.2. «История»**

Дисциплина «История» относится к базовой части математического и естественнонаучного цикла рабочего учебного плана основной образовательной программы по специальности 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

Цель курса: формирование целостного представления об историческом пути России в контексте общемирового исторического развития; развитие патриотического сознания студенчества.

Дисциплина базируется на изученных в школе курсах истории и обществознания.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения дисциплин: Философия, Основы

управленческой деятельности, История защиты информации в РФ и выполнения выпускной квалификационной работы бакалавра.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена во 2 семестре.

### **Б1.Б.3. «Иностранный язык» (английский, французский, немецкий языки)**

Дисциплина «Иностранный язык» относится к базовой части математического и естественнонаучного цикла рабочего учебного плана основной образовательной программы по специальности 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой иностранного языка.

Изучение данной дисциплины базируется на знаниях школьной программы: иностранный язык.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной самостоятельной деятельности в условиях информационного противоборства;

ОК-10: способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

Общая трудоемкость освоения дисциплины составляет 10 зачетных единицы, 360 часов. Преподавание дисциплины ведется на 1 и 2 курсе 2,4 семестр - экзамен, и на 1,2 курсе 1,3 семестр – зачет, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме

тестирования, промежуточная аттестация в форме экзамена во 2 и 4 семестрах и в форме зачета в 1 и 3 семестрах.

Предметом учебного курса является иностранный язык (английский/немецкий) в единстве двух его составляющих - общей, реализующейся как средство международного общения, и специальной, позволяющей осуществлять профессиональную деятельность. Лексический минимум курса составляет 4000 лексических единиц общего и терминологического характера.

Цель курса: формирование умений письменного и устного общения, совершенствование навыков чтения, устной речи, аудирования и письма на иностранном языке, необходимых для выполнения профессиональной деятельности.

Структура курса состоит из четырех частей, соответствующих семестрам обучения. Каждая часть содержит тематический и грамматический модули. При этом в тематических модулях частей I—II преобладают слова и тексты общего характера, начиная с части III - идет углубленное изучение профессиональной тематики и работа с профессионально-ориентированными текстами.

#### **Б1.Б.4. «Экономика»**

Дисциплина «Экономика» относится к базовой части гуманитарного, социального и экономического цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой экономики.

Изучение данной дисциплины базируется на знаниях школьной программы: экономика.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре - экзамен, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена во 2 семестре.

Содержание дисциплины охватывает круг вопросов, связанных со школьным курсом дисциплин: «Обществознание» и «История».

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения дисциплин: Основы управленческой деятельности. Часть 1. Структура и основы деятельности предприятия и выполнения экономического раздела выпускной квалификационной работы бакалавра.

### **Б1.Б.5. «Правоведение»**

Дисциплина «Правоведение» относится к базовой части гуманитарного, социального и экономического цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Дисциплина базируется на ранее полученных знаниях по обществознанию и истории, приобретённых в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-3: способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных юридических понятий, предметов, принципов и специфики основных отраслей отечественного законодательства, изучением вопросов защиты прав и интересов участников конституционных

правоотношений, рассмотрение вопросов, обеспечивающих правовую основу практических умений решения студентами юридических проблем в сфере публичного права.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе, в 1-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: по два текущих контроля успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: история защиты информации, правовая охрана результатов интеллектуальной деятельности.

### **Б1.Б.6. «Основы управленческой деятельности»**

Дисциплина «Основы управленческой деятельности» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется в 2016/2017 учебном году кафедрой управления.

Изучение данной дисциплины базируется на знаниях школьной программы.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 2 курсе, в 3-ем семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 3 семестре.

Курс представляет собой изложение теоретических и практических основ современного менеджмента, рассмотрение основных понятий и направлений управленческой деятельности, принципов обеспечения и организации планирования управления, подходов к принятию управленческих решений.

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.

Структура курса предполагает рассмотрение основных понятий, связанных с управленческой деятельностью, концепций современных теорий управления, методов анализа управления, общей методики принятия управленческих решений.

### **Б1.В.ОД.1 «Психология»**

Дисциплина «Психология» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой прикладной психологии.

Изучение данной дисциплины базируется на знаниях школьной программы. Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе, в 1-ом семестре, продолжительностью 18 недель и предусматривает проведение

учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

Целью изучения дисциплины «Социология» является формирование теоретико-методологических оснований социологического знания и навыков социологического мышления для дальнейшего изучения дисциплин специализации.

В ходе достижения цели решаются следующие задачи:

- изучение основных философских, научных и социально-экономических предпосылок возникновения социологии и основных этапов её развития; сущности основных классических и современных социологических теорий;

- овладение умением использовать понятийный аппарат и методологические принципы основных социологических теорий для научного анализа социальной реальности и собственной социальной практики;

- овладение навыками использования научных социологических источников для изучения общества – учебников, научных журналов, данных социологических исследований и анализа конкретных социальных общностей с помощью понятийного аппарата социологической науки;

- воспитание социальной культуры личности будущего бакалавра.

## **Б1.В.ОД.2. «Русский язык и культура речи»**

Дисциплина «Русский язык и культура речи» относится к базовой части основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой Иностранных языков.

Изучение данной дисциплины базируется на знаниях школьной программы. Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля:



текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета во 2 семестре.

Курс культуры речи нацелен на формирование и развитие у будущего бакалавра - участника профессионального общения комплексной коммуникативной компетенции на русском языке, представляющей собой совокупность знаний, умений, способностей, инициатив личности, необходимых для установления межличностного контакта в социально-культурной, профессиональной (учебной, научной, производственной и др.) сферах и ситуациях человеческой деятельности. Он предполагает знание литературных норм и умение применять их в речи.

Целью курса культуры речи является формирование образцовой языковой личности высокообразованного бакалавра, речь которого соответствует принятым в образованной среде нормам, отличается выразительностью и красотой.

Структура курса предполагает рассмотрение основных понятий, связанных с русским языком и культурой речи.

### **Б1.В.ОД.3. «Социально-психологические основы управленческой деятельности»**

Дисциплина «Социально-психологические основы управленческой деятельности» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой прикладной психологии.

Изучение данной дисциплины базируется на знаниях школьной программы.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-8: способностью определять 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;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2-ом курсе, в 3 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 3 семестре.

Курс содержит основные сведения и базовые знания о предприятиях (организациях) различных форм собственности, включая существующие организационно-правовые формы, в которых может осуществляться их деятельность; дает представление о нормативно-правовых документах, необходимых для создания и функционирования предприятий; позволяет определять наиболее эффективные способы организации и управления предприятиями различных форм собственности.

Целью курса является формирование представлений о сложившемся в экономике России равноправии форм собственности и обеспечении экономической свободы для инициативной хозяйственной деятельности различных организационно-правовых структур в рамках действующего законодательства.

Содержание курса охватывает круг вопросов, связанных с изучением особенностей практической деятельности всех перечисленных в Гражданском кодексе РФ юридических лиц, классифицируемых по основной цели деятельности, организационно-правовой форме и характеру прав, возникающих у их учредителей (участников) в связи с их участием в образовании имущества учреждаемого ими юридического лица.

#### **Б1.В.ОД.4 . «Информационная безопасность кредитно-финансовых операций»**

Дисциплина «Информационная безопасность кредитно-финансовых операций» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: информационная безопасность кредитно-финансовых операций.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ПК-2: современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре - зачет, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

Целью изучения дисциплины является: Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно- финансовых операций; повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной

безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности; Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно-финансовых операций; приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

Дисциплина базируется на ранее изученных дисциплинах: «Правоведение», «Информационные процессы и их безопасность».

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Защита информации в банках», «Защищенный электронный документооборот», «Международные и Российские нормативные акты и стандарты информационной безопасности» и выполнении выпускной квалификационной работы бакалавра.

### **Дисциплины по выбору студентов**

#### **Б1.В.ДВ.1-1. «Системы защиты информации в зарубежных странах»**

Дисциплина «Системы защиты информации в зарубежных странах» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: системы защиты информации в зарубежных странах.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре -зачет, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 6 семестре.

Курс рассматривает вопросы формирования систем и органов защиты информации в ведущих зарубежных странах в общем историческом контексте.

Целью курса является формирование понимания закономерностей становления и тенденций развития систем защиты информации в ведущих зарубежных странах, особенностей их современной организации и функционирования, перспектив развития и возможностях использования зарубежного опыта в России.

Содержание курса раскрывает вопросы, касающиеся формирования и развития систем защиты информации в США, Германии, Великобритании, Франции, Японии, современного опыта организации систем защиты информации в этих странах, правовых основ защиты информации, состава органов защиты информации, особенностей классификации защищаемой информации, а также актуальных направлений международного сотрудничества в области защиты информации.

### **Б1.В.ДВ.1-2. «История защиты информации РФ»**

Дисциплина «История защиты информации» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: история защиты информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-4: способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных,

гуманитарных и экономических наук при решении социальных и профессиональных задач;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре -зачет, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 6 семестре.

Курс рассматривает вопросы становления и развития систем и органов защиты информации в России с XV века по настоящее время в общем историческом контексте.

Целью курса является формирование знаний по закономерностям и тенденциям развития системы защиты информации в России, а также эволюции исторических представлений, взглядов, научных концепций, связанных со структурой и методами защиты информации.

Содержание курса связано с изучением состава защищаемой информации на различных этапах развития государства по видам тайны,

структуры угроз конфиденциальной информации, развития методов несанкционированного доступа к ней, изменения государственной политики в области защиты информации, развития и совершенствования нормативной базы, состава органов защиты информации, направлений и методов обеспечения информационной безопасности, факторов, определяющих современную систему защиты информации.

## **МАТЕМАТИЧЕСКИЙ И ЕСТЕСТВЕННОНАУЧНЫЙ ЦИКЛ** (БАЗОВАЯ ЧАСТЬ)

### **Б2.Б.1. «Математика (математический анализ, алгебра, геометрия)»**

Дисциплина «Математика (математический анализ, алгебра, геометрия)» относится к базовой части математического и естественнонаучного цикла рабочего учебного плана основной образовательной программы по специальности 10.03.01 Информационная безопасность.

Дисциплина реализуется кафедрой математики и естественно-научных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы: математика.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способность логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-2: способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах.

Общая трудоемкость освоения дисциплины составляет 11 зачетных единиц, 396 часов. Преподавание дисциплины ведется на 1-ом и 2-ом курсах, в 1-ом, 2-ом и 3-ем семестрах, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие

виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в каждом семестре.

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами математики: линейная и векторная алгебра, аналитическая геометрия, дифференциальное и интегральное исчисления, теория функций многих переменных, дифференциальные уравнения и ряды.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: теория вероятностей и математическая статистика, математическая логика и теория алгоритмов, дискретная математика, физика.

### **Б2.Б.2. «Теория вероятностей и математическая статистика»**

Дисциплина «Теория вероятностей и математическая статистика» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественно-научных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы: теория вероятностей и математическая статистика.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часа. Преподавание дисциплины ведется на 2-ом курсе, в 3 и 4 семестрах, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 3 семестре и в форме зачета с оценкой в 4 семестре.

**Содержание дисциплины охватывает круг вопросов, связанных со случайными явлениями, которые носят массовый характер и раскрывает основные понятия и теоремы теории вероятностей с**



характеристикой наиболее важных законов распределения случайных величин, применением статистических методов оценивания параметров распределений, владением техникой проверки статистических гипотез.

**Цель курса:** сформировать базовые представления о теории вероятностей и математической статистике под углом зрения их практического приложения в различных областях научных исследований по направлению подготовки.

Содержание курса состоит из двух разделов. В разделе «Теория вероятностей» рассматриваются алгебра событий, вероятностное пространство, основные теоремы теории вероятностей, одномерные случайные величины, числовые характеристики случайных величин, основные распределения случайных величин, многомерные случайные величины и их числовые характеристики, функции случайных величин и предельные теоремы.

В разделе «Математическая статистика» рассматриваются выборочный метод, оценки параметров распределения, статистическая проверка гипотез, теория корреляции, однофакторный дисперсионный анализ, метод статистических испытаний.

### **Б2.Б.3. «Дискретная математика»**

Дисциплина «Дискретная математика» относится к базовой части математического и естественнонаучного профессионального цикла основной образовательной программы подготовки бакалавров по направлению подготовки 10.03.01– Информационная безопасность.

Дисциплина реализуется кафедрой математики и естественно-научных дисциплин.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 3-ем курсе в 5 семестре, продолжительностью 18 недель и предусматривает проведение

учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 5 семестре.

Содержание дисциплины охватывает базовые знания основных понятий дискретной математики и формулировки основных теорем.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при выполнении выпускной квалификационной работы бакалавра.

#### **Б2.Б.4 «Физика»**

Дисциплина «Физика» относится к базовой части математического и естественнонаучного цикла рабочего учебного плана основной образовательной программы по специальности 10.03.01 Информационная безопасность.

Дисциплина реализуется кафедрой математики и естественно - научных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы математики и физики.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-8: способностью определять 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;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2-ом курсе, в 3-ем семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены

следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 3-ем семестре.

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами физики: механика, молекулярная физика и термодинамика, электродинамика, оптика, так и с современными: специальная теория относительности, квантовая механика и изложение на их основе элементов квантовой оптики, а атомной и ядерной физики, а также элементов физики твердого тела.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: теоретическая механика, электротехника и электроника, химия.

### **Б2.Б.5 «Информатика»**

Дисциплина «Информатика» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: информатика.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Преподавание дисциплины ведется на 1-ом курсе, в 1-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля:

текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 1 семестре.

**Курс освещает вопросы, связанные с систематизацией теоретических знаний и практических приемов создания, хранения, обработки и передачи информации с использованием средств вычислительно-коммуникационной техники.**

**Целью курса является изучение теоретических основ информатики, приобретение практических знаний в области использования автоматизированных информационных систем.**

**Содержание курса охватывает вопросы изучения основных понятий информатики (информация, автоматика, информационные процессы, системы и технологии); аспектов моделирования и представления информации и алгоритмизации информационных процессов; сущности и классификации информационных технологий; базовых информационно-коммуникационных технологий обработки и передачи информации. В прагматическую составляющую курса включены вопросы изучения: способов представления и преобразования информации в вычислительных системах, в том числе, структур их файловых систем; использования и настройки интерфейса операционных систем; основ работы с универсальными пакетами офисных приложений - текстового процессора, электронных таблиц и презентаций; способов обмена данными между приложениями; интерфейса и принципов работы систем управления базами данных; способов коммуникации, навигации и поиска информации в распределенных информационно- вычислительных сетях.**

### **Б2.Б.6 «Теория информации»**

Дисциплина «Теория информации» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 2-ом курсе, во 3-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 3 семестре.

**Курс освещает вопросы, связанные с теоретическими и практическими аспектами теории информации, в частности с формированием практических навыков по применению методов теории информации для защиты информации в компьютерных системах.**

**Целью курса является приобретение навыков работы с понятиями теории информации и её использования в информационной безопасности; формирование умения применять алгоритмы эффективного, помехозащищенного и криптографического кодирования; формирование понимания сути информационных процессов в системах передачи, хранения и преобразования данных.**

**Содержание курса охватывает основные понятия теории информации, необходимые для использования защиты информации в компьютерных системах, а именно: понятие информации, подходы к измерению информации, свойства меры информации, характеристики канала связи, понятие кодирования, алгоритмы кодирования (эффективное кодирование, помехозащищенное кодирование, криптографическое кодирование). Рассматриваются коды Шенона-Фэно, Хаффмана, блочные помехозащищенные коды, совершенные и квазисовершенные помехозащищенные коды; вопросы шифрования с симметричным и несимметричным ключом.**

## **Вариативная часть Дисциплины, рекомендуемые ФГОС**

### **Б2.В.ОД.1. «Математическая логика и теория алгоритмов»**

Дисциплина «Математическая логика и теория алгоритмов» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественно-научных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы: математическая логика и теория алгоритмов.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2-ом курсе, 4-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 4 семестре.

**Курс рассматривает основные понятия математической логики и теории алгоритмов как основы математических методов обработки информации в вычислительной технике.**

**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.**

**Содержание курса включает рассмотрение вопросов исчисления высказываний, предикатов, вычислимости функций, решения диофантовых уравнений, решения задач комбинаторной оптимизации, а также рассмотрение проблематики решения NP- полных задач.**

## **Б2.В.ОД.2. «Физическая защита информационных объектов»**

Дисциплина «Физические основы защиты информации» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: физические основы защиты информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-08: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 3-ем курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 5 семестре.

**Курс рассматривает волновые процессы в их прикладном значении для защиты информации.**

**Курс направлен на формирование понимания физической природы волновых процессов в различных средах и возможности использования законов физики для обеспечения защиты информации.**

**Курс состоит из двух разделов. В первом разделе рассматриваются электромагнитные волны, физическая картина излучений, дается представление об экранировании и электромагнитной совместимости, побочных электромагнитных излучениях и наводках (ПЭМИН). Во втором разделе изучаются упругие волны, основы акустики речи и акустики помещений, инфразвук, ультразвук, а также физические поля как носители информации об объектах.**

### **Б2.В.ОД.3. «Информационные процессы (системы) и их безопасность»**

Дисциплина «Информационные процессы (системы) и их безопасность» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: информационные процессы (системы) и их безопасность.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-22 способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики;

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 2-ом курсе, в 3-ем и в 4-ом семестрах, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 4 семестре и в форме зачета в 3 семестре.

**Курс освещает вопросы, связанные с теорией и практикой исследования и реализации (использования) информационных процессов и систем в современном обществе.**

**Целью курса является формирование понимания особенностей анализа, синтеза и функционирования информационных систем, приобретение навыков и умений исследования и использования информационных систем по профилю деятельности.**

**Содержание курса включает современные концепции (теории) информации, методы её исследования, модели динамики изменений объективной реальности (времени), сущность и классификацию информационных процессов, аспекты их моделирования и алгоритмизации, характеристики и классификации информационных систем, их проектирование и использование в конкретных предметных**



областях, а также общие аспекты безопасности информационных процессов и систем. Особое внимание обращено на кибернетические и интеллектуальные системы. Излагаются основные парадигмы теории интеллектуальных систем, включая так называемые системы «искусственного интеллекта». Рассматриваются инструментальные средства исследования, моделирования и проектирования информационных процессов и систем.

#### **Б2.В.ОД.4. «Концепции современного естествознания»**

Дисциплина «Концепции современного естествознания» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественно-научных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы: концепция современного естествознания.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля:

текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета во 2 семестре.

### **Б2.В.ОД.5. «Пакеты прикладных программ»**

Дисциплина «Пакеты прикладных программ» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: пакеты прикладных программ современного офиса.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой во 2 семестре.

**Курс направлен на профессиональное освоение существующих пакетов прикладных программ современного офиса (на примере Microsoft Office), а также способов оптимального решения повседневных**

деловых задач с использованием средств автоматизации на основе вышеупомянутого пакета.

Целью курса является развитие у студентов теоретических знаний в области использования прикладного программного обеспечения и формирование умений и практических навыков, необходимых для успешного применения в профессиональной деятельности полной конфигурации офисного пакета Microsoft Office 2003-2010.

Содержание курса охватывает основные задачи офисной деятельности и технологии их решения, проблему выбора и адаптации Пакета прикладных офисных программ к конкретным задачам заданной предметной области. Детально изучаются базовые компоненты пакета Microsoft Office 2003-2010 (текстовый и табличный процессор, средства презентаций, система управления базой данных, почтовая служба и деловой органайзер, средства управления вводом-выводом, распознаванием и обработкой мультимедийной информации), его основные возможности, принципы и приемы разработки и использования различных классов OLE-связанных документальных материалов (деловая переписка, планирующие и отчетные документы, учебно-методические и научные работы). В дополнение к пакету Microsoft Office затрагиваются офисные средства телекоммуникаций и IP-телефонии (ICQ, Skype) и OCR (FineReader), системы машинного перевода (локальные и сетевые сервисы), Интернет-технологии поиска и управления коллективными информационными ресурсами, системы управления проектами.

### **Б2.В.ДВ.1-1. «Операционные системы, среды и оболочки»**

Дисциплина «Операционные системы, среды и оболочки» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: операционные системы, среды и оболочки.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2-ом курсе, в 4 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 4 семестре.

**Курс освещает вопросы, связанные с теоретическими и практическими аспектами функционирования современных операционных систем и оболочек, а также формированием практических навыков по настройке и администрированию встроенных средств защиты информации операционных систем (ОС).**

**Целью курса является приобретение понимания архитектуры и внутреннего устройства современных ОС, знакомство с базовыми элементами графического и консольного интерфейсов, получения навыков выбора и реализации безопасных конфигураций систем, как в автономном, так и в сетевом исполнении.**

**Содержание курса охватывает вопросы эволюции и развития операционных систем и оболочек, архитектуры, реализации функций, возлагаемых на ОС, в части обеспечения пользовательского интерфейса и интерфейса к аппаратной платформе, поддержки многозадачности, распределения ресурсов между конкурентными процессами, организацию виртуальной памяти и файловой системы, взаимодействия между процессами. Отдельным блоком рассматриваются вопросы, относящиеся к подсистеме защиты информации. Подробно изучаются компоненты, реализующие базовые сервисы безопасности, такие как аутентификация пользователей, разграничение доступа к защищаемым ресурсам и регистрация событий.**

## **Б2.В.ДВ.1-2. «Базы данных, системы управления базами данных»**

Дисциплина «Базы данных, системы управления базами данных» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: базы данных, системы управления базами данных.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2-ом курсе, в 4 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 4 семестре.

**В курсе излагаются основные понятия и методы организации реляционных баз данных и манипулирования ими, а также описываются базовые подходы к проектированию реляционных баз данных. Важную часть курса составляют вопросы защиты информации в базах данных.**

**Целью курса является формирование понимания основных принципов реляционной модели данных, навыков проектирования систем управления базами данных с использованием диаграммных моделей.**

**В курсе рассматриваются основные понятия реляционной модели данных, структурная, манипуляционная и целостная составляющие модели. Изучаются важные аспекты теории баз данных, связанные с функциональными зависимостями, процесс проектирования реляционных баз данных, на основе принципов нормализации, а также подходы к проектированию реляционных баз данных с использованием диаграммных семантических моделей данных. Также рассмотрены вопросы формирования запросов к базе данных и основные элементы языка SQL. Изучается общая концепция защиты информации, в частности вопросы определения прав и привилегий пользователей.**

### **Б2.В.ДВ.2-1. «Основы алгоритмизации и программирования»**

Дисциплина «Основы алгоритмизации и программирования» относится к базовой части основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях, полученных в рамках изучения ООП «Информационная безопасность»: дисциплина информатика.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение

учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета во 2 семестре.

Цель дисциплины состоит в изучении методов алгоритмизации, основ программирования на алгоритмических языках высокого уровня и в использовании полученных навыков при решении инженерных задач.

Задачи курса:

- формирование базовых знаний по алгоритмизации и программированию - о стиле написания программ, о рациональные методах их разработки и оптимизации, о стратегии отладки и тестирования программ;

- получение базового уровня по программированию на языке Си с использованием простых типов данных: базовых типов данных и массивов;

- изучение структур данных в памяти и в файлах и алгоритмов работы с ними с использованием языка Си;

- знакомство с основными принципами организации хранения и поиска данных, алгоритмами сортировки и поиска;

- приобретение навыков использования базового набора фрагментов и алгоритмов в процессе разработки программ, навыков анализа и “чтения” программ;

- изучение основ технологии программирования и методов решения вычислительных задач и задач обработки символьных данных;

- формирование уровня знания языка, позволяющего свободно оперировать типами данных и переменными произвольной сложности и модульными алгоритмами их обработки.

## **Б2.В.ДВ.2-2. «Пакеты прикладных математических программ»**

Дисциплина «Пакеты прикладных математических программ» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: пакет прикладных математических программ.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, во 2-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета во 2 семестре.

**Курс направлен на изучение существующих пакетов прикладных математических программ и на этой основе освоение эффективных способов решения задач обеспечения информационной безопасности.**

**Целью курса является формирование практических навыков использования современных пакетов прикладных математических программ при проведении расчетного и имитационного моделирования информационных процессов и систем в прикладных задачах информационной безопасности.**

**Содержание курса включает обзор наиболее популярных специализированных и универсальных пакетов прикладных математических программ, математических пакетов с открытым кодом и интегрированных пакетов системного моделирования; основные подходы к организации интерфейса и реализации командных языков; функциональные возможности и предназначение пакетов; основные вычислительные процедуры, реализуемые изучаемыми программными средствами; аспекты теоретико-вероятностного моделирования процессов и систем; синтез и манипулирование теоретико-графовыми объектами; мультимедийная визуализация математических моделей; имитационно-функциональное моделирование сложных систем.**

## **ПРОФЕССИОНАЛЬНЫЙ ЦИКЛ**

(БАЗОВАЯ ЧАСТЬ)

### **БЗ.Б.1. «Основы информационной безопасности»**

Дисциплина «Основы информационной безопасности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».



Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: основы информационной безопасности.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 1-ом и 2-ом курсе во 2-ом и в 3-ем семестрах, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета во 2 семестре и в форме экзамена в 3 семестре.

**Содержание дисциплины охватывает круг 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.**

**Целью курса является формирование знаний о совокупности проблем 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.**

**В курсе изучаются понятийный аппарат и базовые положения законодательных и нормативных документов по информационной безопасности; рассматриваются сущность и содержание информационной безопасности, её место в системе национальной безопасности, основные требования по обеспечению информационной**

**безопасности государства, общества, личности; раскрываются объекты безопасности, состав защищаемой информации, структура угроз информации, средства обеспечения безопасности, направления, виды и методы деятельности по обеспечению информационной безопасности, а также основные задачи государственной системы (органов) защиты информации.**

### **Б3.Б.2. «Аппаратные средства вычислительной техники»**

Дисциплина «Аппаратные средства вычислительной техники» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: аппаратные средства вычислительной техники.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 5 семестре.

**Предметом учебного курса являются вопросы, связанные с устройством и функционированием аппаратных средств вычислительной техники.**

**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.**

**Содержание курса охватывает следующие вопросы: арифметические и логические основы цифровых машин, элементы и узлы ЭВМ, принцип программного управления и микропроцессоры, периферийные устройства ЭВМ, архитектура и принцип работы ПЭВМ, основы построения компьютерных сетей.**

### **Б3.Б.3. «Программно-аппаратные средства защиты информации»**

Дисциплина «Программно-аппаратные средства защиты информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: программно-аппаратные средства защиты информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-1: способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы

безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 7 семестре и курсовой работы в 7 семестре.

**Предмет курса - механизмы и практические методы защиты информации в автономных и распределенных компьютерных системах.**

**Цель курса - формирование знаний о современных средствах защиты информации в компьютерных системах, овладение методами решения профессиональных задач, умения ориентироваться в продуктах и тенденциях развития средств защиты информационных технологий.**

**В рамках курса рассматриваются основные понятия программно-аппаратной защиты информации, уязвимости компьютерных систем, политики безопасности в компьютерных системах, вопросы оценки защищенности, базовые сервисы безопасности (идентификация и аутентификация субъектов доступа, регистрация событий и аудит, механизмы контроля целостности информации), функции безопасности ОС WINDOWS, функции безопасности ОС UNIX, разграничение доступа в СУБД, особенности защиты информации в распределенных системах, аппаратно-программные средства защиты информации (СЗИ и СКЗИ «Secret Net»), средства аппаратной поддержки (смарт-карты, гмб-токены и т.п.), сетевые угрозы, уязвимости и атаки, средства обнаружения уязвимостей, межсетевые экраны, виртуальные частные сети (VPN), безопасность уровня сетевого взаимодействия.**

#### **Б3.Б.4. «Криптографические методы защиты информации»**

Дисциплина «Криптографические методы защиты информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: криптографические методы защиты информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 7 семестре.

**В курсе в систематизированном виде излагаются вопросы обеспечения безопасности каналов передачи информации, систем электронных платежей, электронного документооборота с использованием криптографических методов.**

**Целью курса является приобретение знаний о базовых криптографических системах и схемах, их основных параметрах и умений применять на практике имеющиеся криптографические средства.**

**Содержание курса охватывает общетеоретические вопросы криптографической защиты информации и практики применения ее методов и средств в современных информационных системах, синтеза и анализа криптографических протоколов, закономерности построения сложных криптосистем, а также конкретные виды базовых криптографических протоколов и схем, получивших широкое применение в качестве инструментария для создания систем электронных платежей и систем документооборота в электронной коммерции.**

### **Б3.Б.5. «Организационное и правовое обеспечение информационной безопасности»**

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части профессионального цикла основной

образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: организационно и правовое обеспечение информационной безопасности.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;

ПСК-3: способен разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение;

ПСК-4: способен организовать контроль защищенности объектов в соответствии с нормативными документами.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Преподавание дисциплины ведется на 2 курсе, в 4 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля:

текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 4 семестре и курсовой работы в 4 семестре.

**Курс охватывает круг вопросов, связанных с целями, функциями и структурой правового обеспечения информационной безопасности и обеспечивающих ее мер и средств правовой защиты информации, структурой законодательства в информационной сфере.**

**Целью курса (1 часть) 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.**

**Целью курса (2 часть) 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.**

**Содержание курса (1 часть) раскрывает информационная сферу как объект правовых отношений, дает понятие тайны (государственной, коммерческой, служебной, профессиональной), как правового режима ограничения доступа к информации, рассматривает особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан, а также основные положения гражданского законодательства о правах на результаты интеллектуальной деятельности и средства индивидуализации, правовые нормы сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации, вопросы о Курс освещает вопросы, связанные с теоретическими и практическими проблемами создания и функционирования систем организационного обеспечения информационной безопасности, а также формированием практических навыков по организационной защите информации, рассматриваются вопросы определения стратегических целей организационного обеспечения информационной безопасности, основанное на анализе внутренних и внешних факторов угроз; установление приоритетов и последовательности решения задач, привлечение и распределение ресурсов организации, основанные на методах программно-целевого планирования.**

**Содержание курса (2 часть) предусматривает изучение сущности организационного обеспечения информационной безопасности, 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**

**По тематике дисциплины предусмотрено выполнение курсовых работ.**

### **Б3.Б.6. «Техническая защита информации»**

Дисциплина «Техническая защита информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: техническая защита информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-17);

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18);

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики (ПСК-1);

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные



консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 5 семестре.

**В курсе освещены вопросы, связанные с анализом возможных технических каналов утечки информации и защиты объектов информатизации техническими способами и средствами, в том числе, проведение специальных исследований, обследований и специальных проверок.**

**Целью курса является рассмотрение возникновения технических каналов утечки информации и возможности защиты информации техническими средствами.**

**В курсе рассматриваются объекты информационной защиты, виды угроз информации, вопросы образования технических каналов утечки информации, способы преднамеренного воздействия на информацию, способы добывания информации злоумышленником, методы и способы защиты информации техническими средствами защиты.**

**По тематике дисциплины предусмотрено выполнение курсовой работы.**

### **Б3.Б.7. «Сети и системы передачи информации»**

Дисциплина «Сети и системы передачи информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: сети и системы передачи информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 6 семестре.

**Курс ориентирован на теоретическое изучение и практическое освоение принципов построения и применения современных сетей и систем передачи данных.**

**Целью курса является формирование знаний в области выбора, анализа и применения сетей и систем передачи данных.**

**Содержание курса охватывает основные понятия и определения передачи информации, эталонную модель взаимодействия открытых систем (модель ISO/OSI), модель TCPDP, архитектуру и средства взаимодействия процессов в сетях, основные принципы построения и современные тенденции развития сетей. Рассматривается архитектура и топологии построения современных ЛВС, технологии Ethernet (FastEthernet, GigabitEthernet), TokenRing, FDDI - стандарты, принципы работы, сравнительные характеристики, преимущества и недостатки, основные средства построения современных ЛВС, классификации, внутренняя архитектура, режимы работы, протоколы сетевого уровня модели ISO/OSI. Изучаются основы организации и функционирования, архитектура и принципы построения сети Internet, протоколы маршрутизации, кроме того - мультисервисные сети, особенности построения таких сетей, технологии передачи голосового трафика VoIP, IP-телефония.**

### **БЗ.Б.8. «Безопасность жизнедеятельности»**

Дисциплина «Безопасность жизнедеятельности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления качеством и стандартизации.

Изучение данной дисциплины базируется на знаниях школьной программы: безопасность жизнедеятельности.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-17);

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, в 1 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

Целью изучения дисциплины является: Формирование профессиональной культуры безопасности, под которой понимается готовность и способность личности использовать в профессиональной деятельности приобретенную совокупность знаний, умений и навыков для обеспечения безопасности в сфере профессиональной деятельности. Формирование, развитие и закрепление у студентов сложившихся в науке теоретических знаний и практических навыков, необходимых для оценки негативных воздействий среды обитания естественного, техногенного и антропогенного происхождения. Разработка и реализация мер защиты человека от негативных воздействий; знание правового регулирования безопасности жизнедеятельности; основ управленческой деятельности для обеспечения устойчивости функционирования объектов и технических систем в штатных и чрезвычайных ситуациях.

Дисциплина «Безопасность жизнедеятельности» базируется на знаниях, полученных в процессе изучения программы общеобразовательной школы.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения дисциплин: Охрана труда и выполнения выпускной квалификационной работы бакалавра.

### **Б3.Б.9. «Языки программирования»**

Дисциплина «Языки программирования» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: языки программирования.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 2 курсе, в 4 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 4 семестре.

**Курс направлен на изучение объектно-ориентированных языков программирования семейства С (С++, С#) и охватывает круг вопросов, связанных с понятиями объектно-ориентированного программирования, абстрактного типа данных, объекта, метода, функции, наследования, инкапсуляции, класса, конструкторов и деструкторов, потоков ввода-вывода, виртуальных функций.**

**Целью курса является формирование компетенций в области использования современных промышленных языков программирования и средств разработки программного обеспечения для решения прикладных задач информационной безопасности на базе объектно-ориентированного подхода.**

**Содержание курса охватывает особенности объектно-ориентированных языков программирования, их достоинства и недостатки; включает основные элементы С++ (базовые структуры и типы данных, виды доступа, классы и объекты, техника указателей, базовые классы и указатели, производные классы: иерархия наследования, виртуальные функции и абстрактные классы, динамическое распределение памяти, потоки ввода / вывода, конструкторы и деструкторы, функции-друзья, обобщение операторов определения), и механизмы их использования (работа с файлами, вызов**

**конструкторов функций оператора сложения, конверсия, программирование команд меню); отражает современные тенденции в развитии языка C++ (универсальные платформы Microsoft.NET и технологии программирования Microsoft.NET Framework) и характерные особенности языка C# (система типов, делегаты, события, интерфейсы, атрибуты, механизм сериализации и классы-коллекции).**

### **Б3.Б.10. «Технологии и методы программирования»**

Дисциплина «Технологии и методы программирования» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на знаниях школьной программы: технологии и методы программирования.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-6: способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 5 семестре.

Курс направлен на изучение современных методов и технологий программирования, поддерживающих процесс программирования на всех этапах конструирования и жизненного цикла программной системы (ПС) и базирующихся на методологии структурного анализа и проектирования программных средств и объектно-ориентированного анализа предметной области.

Целью курса является формирование компетенций студентов в области основных технологий и методов программирования, применяемых при разработке современных ПС; усвоение теоретических знаний, связанных с проектированием, спецификацией, разработкой, тестированием и отладкой ПС, а также документированием приложений; приобретение практических навыков в области использования технологий программирования (кодирование, отладка и тестирование) в конкретных приложениях; формирование представлений о принципах и методах программирования в современных языках: модульности, структурности, композиции и декомпозиции.

Содержание курса охватывает следующие основные вопросы: модели жизненного цикла ПС, спецификация программ, структурный подход к проектированию ПС, модульное программирование, основные характеристики и организация программного модуля, нисходящий и восходящий методы конструирования ПС, разработка интерфейса пользователя, тестирование ПС, автономная и комплексная отладка ПС, показатели качества ПС, основные парадигмы и методы программирования, эволюция языков программирования, методы представления знаний и данных в ПС, абстрагирование типов и инкапсуляция, полиморфизм, перекрытие и перегрузка методов, внутренняя организация объекта, таблицы динамических и виртуальных методов, технологии документирования и стандартизации ПС, современные CASE-технологии проектирования ПС, системы UML-моделирования.

### **Б3.Б.11. «Управление информационной безопасностью»**

Дисциплина «Управление информационной безопасностью» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях, полученных в результате ранее изученных дисциплин: «Введение в профессию», «Основы информационной безопасности» и др..

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;

ПСК-2: способен формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-4: способен организовать контроль защищенности объектов в соответствии с нормативными документами.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

**Содержание дисциплины охватывает вопросы, связанных с изучением сущности и стандартных процедур управления безопасностью объектов информационной инфраструктуры, анализом методов и систем управления информационной безопасностью, требований к аудиту систем управления защитой информации.**

**Целью курса является формирование знаний по основам управления**

**информационной безопасностью предприятия (организации) и методам повышения эффективности системы управления безопасностью объекта информатизации.**

**Структура курса раскрывает требования международных и российских стандартов по информационной безопасности, классификацию систем управления, меры и средства управления**

**информационной безопасностью, этапы внедрения систем управления, а также аудит и оценку эффективности систем управления информационной безопасностью предприятия (организации).**

**По тематике дисциплины для профиля «Организация и технология защиты информации» предусмотрено выполнение курсовой работы.**

### **Б3.Б.12. «Документоведение»**

Дисциплина «Документоведение» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на знаниях школьной программы: документоведение.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ПК-8: способностью определять 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;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1 курсе, во 2 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

**Содержание курса раскрывает вопросы, связанные с документированием правовой, управленческой, экономической, социальной, технической и научной информации, формированием систем документации, защитой документированной информации, а также основами документационного обеспечения управления.**



**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.**

**Структура курса предполагает 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.**

### **БЗ.Б.13. «Электротехника»**

Дисциплина «Электротехника» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: дисциплина «физика».

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 2 курсе, в 4 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 4 семестре.

**Курс охватывает вопросы, связанные с анализом и расчетом электрических цепей различной сложности, а также изучением**

современных методов расчета электрических цепей, основанных на компьютерных технологиях.

Целью курса является формирование понимания аналитических и машинных методов расчета электрических цепей, изучение физических явлений и эффектов, имеющих в современной электронной аппаратуре и их учета при защите информации.

Курс объединяет ряд логически связанных разделов. Первый - базируется на разделе «электростатика» курса физики, и раскрывает методы расчета электрических цепей постоянного тока. Во втором и третьем разделах рассматриваются цепи переменного тока с синусоидальными и импульсными источниками. В последующих разделах анализируются цепи с нелинейными и многополюсными элементами (диоды, транзисторы, операционные усилители), применяемыми в современной электронной аппаратуре.

#### **Б3.Б.14. «Электроника и схемотехника»**

Дисциплина «Электротехника и схемотехника» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях, полученных в результате ранее изученных дисциплин: «Физика», «Введение в профессию», «Основы информационной безопасности» и др..

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-8: способностью определять 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;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия,

самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 5 семестре.

**Курс охватывает вопросы, связанные 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.**

**Целью курса является изучение принципов действия и особенностей применения типовых аналоговых и цифровых электронных устройств в современных технических средствах.**

**Курс объединяет ряд разделов. Первый раздел вводит в основы современной полупроводниковой электроники. Во втором разделе рассматриваются полупроводниковые приборы - транзисторы. В третьем разделе изучаются усилительные схемы, принципы и особенности их работы. В четвертом разделе изучается операционный усилитель, применяемый в различных областях схемотехники. В последнем разделе рассмотрено применение транзисторов в цифровой технике.**

### **БЗ.Б.15. «Информационные технологии»**

Дисциплина «Информационные технологии» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях, полученных в результате ранее изученных дисциплин: «Физика», «Введение в профессию», «Основы информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 5 семестре.

**Курс ориентирован на теоретическое изучение и практическое освоение основных классов современных информационно-коммуникационных технологий по осваиваемым профилям подготовки.**

**Целью курса является формирование компетенций в области выбора, адаптации, использования и синтеза информационно-коммуникационных технологий, обеспечивающих функционирование информационных систем в рамках заданной политики безопасности.**

**Содержание курса охватывает классы современных компьютерных (автоматизированных) информационно-коммуникационных технологий общего назначения, в том числе, управления и принятия решений, системного анализа, формирования и использования коллективных источников знаний, массовых вычислений и моделирования, проектирования и разработки информационных систем, поддержки образовательного процесса и научных исследований.**

## **Вариативная часть Дисциплины, рекомендуемые ФГОС**

### **Б3.В.ОД.1. «Основы исследований информационной безопасности»**

Дисциплина «Основы исследований информационной безопасности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности. Изучение данной дисциплины базируется на знаниях, полученных в результате ранее изученных дисциплин: «Физика», «Введение в профессию», «Основы информационной безопасности» и др..

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-8: способностью определять 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;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 1-ом курсе, в 1-ом семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 1 семестре.

Целью изучения дисциплины является формирование у студентов понимания роли и места научной деятельности для выбранной профессии, а также получение первичных навыков научных исследований с учётом особенностей обучения и решения специфических теоретических и практических задач в области информационной безопасности.

Основными задачами дисциплины являются: подготовка студентов к грамотному выполнению заданий по специальным дисциплинам и к участию в научно-исследовательских работах, проводимых на кафедре, факультете и академии; ознакомление студентов со спецификой и методологией научной деятельности; ознакомление студентов с математическими и аналитическими методами, применяемыми в научных исследованиях, способами их организации и проведения, а также оформления полученных результатов; осознание тесной взаимосвязи деятельности в области информационной безопасности с научными исследованиями.

Дисциплина базируется на одновременно изучаемых дисциплинах: “Математический анализ”, “Физика”, ”Введение в профессию“, “Основы информатики “, «Основы информационной безопасности» и следующих компетенциях: ОК-1, 2, 4 и ПК - 1, 5, 13, 19.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин профессионального цикла (базовой и вариативной частей) и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ОД.2. «Информационная безопасность предприятий»**

Дисциплина «Информационная безопасность предприятий» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях, полученных в результате ранее изученных дисциплин: «Физика», «Введение в профессию», «Основы информационной безопасности» и др..

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики;

ПСК-2: способен формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

ПСК-3: способен разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение;

Общая трудоемкость освоения дисциплины составляет 8 зачетных единиц, 288 часов. Преподавание дисциплины ведется на 4 курсе, в 7 и 8 семестрах, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 8 семестре и в форме зачета в 7 семестре и курсовой работы в 8 семестре.

Целями изучения дисциплины являются: Дать студентам знания по организации целесообразных мероприятий по защите информации на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных требований в области теории обеспечения информационной безопасности на основе комплексного подхода. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий защиты информации на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных международных и отечественных стандартов информационной безопасности. Дисциплина базируется на ранее изученных дисциплинах: «Организационно-правовое обеспечение информационной безопасностью», «Управление информационной безопасностью», «Экономические аспекты защиты информации».

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин профессионального цикла «Аттестация объектов информатизации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Организация защиты персональных данных на предприятии» и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ОД.3. «Защищенные информационные технологии»**

Дисциплина «Защищенные информационные технологии» относится к базовой части математического и естественнонаучного цикла основной образовательной программы подготовки студентов по направлению 090900.62 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Информационные технологии», «Теория информации», «Техническая защита информации».

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 5 семестре.

**Курс ориентирован на теоретическое изучение и практическое освоение основных классов современных информационно-коммуникационных технологий.**

**Целью курса является формирование компетенций в области выбора, адаптации, использования и синтеза информационно-коммуникационных технологий, обеспечивающих функционирование информационных систем в рамках заданной политики безопасности.**

**Содержание курса охватывает существующие программные продукты и защищенные технологии финансовых структур и менеджмента предприятий и организаций. Защитные мероприятия в структуре городского хозяйства и различных ситуационных центров. Особенности защиты интеллектуальной собственности в различных информационных ресурсах. Технология применения ЭЦП и др. активных средств противодействия утечки информации и подслушивания. Методология применения цифровых водяных знаков в организации защиты информационных объектов и документов на предприятии.**



### **Б3.В.ОД.4. «Международные и российские нормативные акты и стандарты по информационной безопасности»**

Дисциплина «Международные и российские нормативные акты и стандарты по информационной безопасности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Организационно - правовое обеспечение информационной безопасности», «Основы информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПСК-4: способен организовать контроль защищенности объектов в соответствии с нормативными документами.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 7 семестре.

**Курс посвящен проблеме обеспечения безопасности информационных систем в части задачи нормативного регулирования деятельности в этой области.**

**Цель курса - ознакомить с отечественными и зарубежными нормативными актами и иными документами в области обеспечения безопасности информационных систем и смежных областях, дать представление о практических навыках проведения аудита систем и организаций на соответствие нормативным актам.**

Содержание курса включает с себя вопросы, связанные со структурой и содержанием процесса обеспечения безопасности информационных систем. Рассматриваются задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структура и содержание системы нормативного обеспечения безопасности. Раскрываются вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем, нормативного обеспечения в области анализа рисков нарушения безопасности, нормативного регулирования технической и криптографической защиты информации. Рассмотрены стандарты в области обеспечения функциональной безопасности информационных систем, организации проектирования информационных систем в защищённом исполнении, управления информационной безопасностью, тенденции развития системы нормативного обеспечения безопасности.

#### **Б3.В.ОД.5. «Информационно-аналитическая деятельность по обеспечению комплексной безопасности»**

Дисциплина «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплин: «Организационно-правовое обеспечение информационной безопасности», «Основы информационной безопасности» и др. информационно-аналитическая деятельность по обеспечению комплексной безопасности.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной самостоятельной деятельности в условиях информационного противоборства;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПСК-2: способен формировать предложения по оптимизации функционального процесса и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 8 семестре.

**Содержание дисциплины связано с изучением сущности и значения информационно-аналитической деятельности для обеспечения защиты информации, ее места в системе информационной безопасности, определением теоретических, концептуальных, методологических, организационных и правовых основ информационно-аналитического обеспечения управления.**

**Целью курса является формирование умений осуществлять эффективную информационно-аналитическую деятельность по обеспечению информационной безопасности предприятия, включающую организацию целенаправленного поиска, оценки и анализа информации.**

**Структура курса знакомит с современными методами и организацией аналитической работы, технологией и средствами поиска, сопоставления, отбора, оценки (актуальности, достоверности и др.) информации для обеспечения безопасности предприятия (организации).**

### **Б3.В.ОД.6. «Инженерно-техническая защита информации»**

Дисциплина «Инженерно-техническая защита информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: и ранее изученных дисциплин: «Аппаратные средства вычислительной техники», «Программно-аппаратные средства вычислительной техники», «Техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 7 семестре.

**В курсе рассматриваются вопросы построения систем защиты информации на объектах информатизации, с использованием технических способов и средств.**

**Целью курса является формирование знаний по организации систем технической защиты информации на различных объектах.**

**Содержание курса охватывает вопросы организации работ по созданию системы технической защиты информации на объекте, определением объемов и задач на каждом этапе её разработки, проведению необходимых мероприятий по выявлению технических каналов утечки информации и преднамеренного воздействия на защищаемую информацию, выбору способов и мер по блокированию этих каналов. Изучаются способы съема информации злоумышленником с помощью специальных электронных устройств и организация соответствующих защитных мероприятий.**

### **Б3.В.ОД.7. «Технические средства охраны»**

Дисциплина «Технические средства охраны» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: и ранее изученных дисциплин: «Аппаратные средства

вычислительной техники», «Программно-аппаратные средства вычислительной техники» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 7 семестре.

**В курсе рассматриваются вопросы организации охраны объекта техническими средствами тревожной сигнализации, системами контроля и управления доступом.**

**Целью курса является формирование знаний в области защиты объектов информатизации техническими средствами охраны.**

**Содержание курса охватывает вопросы классификации объектов охраны, категорирования объектов, требований к защищенности объектов и их элементов (строительным конструкциям), оборудования территории, здания, помещения техническими средствами охранно-пожарной сигнализации, телевизионной системой видеонаблюдения, системами контроля и управления доступом на объект.**

**Курс базируется на изучении требований стандартов, а также нормативных документов МВД России, МЧС России, МО России.**

### **Б3.В.ОД.8. «Информационная безопасность автоматизированных систем»**

Дисциплина «Информационная безопасность автоматизированных систем» относится к базовой части профессионального цикла основной

образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: и ранее изученных дисциплин: «Аппаратные средства вычислительной техники», «Программно-аппаратные средства вычислительной техники», «техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной самостоятельной деятельности в условиях информационного противоборства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 7 семестре.

**Курс охватывает круг вопросов, связанных с проблематикой разработки и развития методов обеспечения информационной безопасности автоматизированных систем, а также выбором эффективных механизмов для их реализации.**

**Цель курса - 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.**

**Содержание курса включает 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, антивирусная защита, обнаружение вторжений, межсетевое экранирование, виртуализация как механизм защиты информации в сетях; элементы криптографической защиты; основы безопасности программного обеспечения; вопросы организации обеспечения информационной безопасности систем: нормативная база, структура и принципы построения системы обеспечения информационной безопасности, рубежи защиты систем и связанные с ними задачи, виды и этапы обеспечения информационной безопасности, элементы управления информационной безопасностью автоматизированных систем.**

**По тематике дисциплины для профиля «Комплексная защита объектов информатизации» предусмотрено выполнение курсовых работ.**

### **Б3.В.ОД.9. «Защита и обработка конфиденциальных документов»**

Дисциплина «Защита и обработка конфиденциальных документов» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы, «Документоведение», «Организационно-правовое обеспечение информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 5 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 5 семестре.

**Предмет изучения курса - проблемы построения и совершенствования технологии защищенного документооборота в условиях применения разнообразных типов носителей документной информации (бумажных, электронных и др.), а также различных средств, способов и систем обработки и хранения конфиденциальных документов.**

**Цель курса - формирование знаний по научным, прикладным и методическим аспектам организации выполнения технологических стадий, процедур и операций с конфиденциальными документами, проектирование рациональной технологической схемы защищенного документооборота.**

**Тематика курса объединена в ряд логически связанных разделов. Первый носит теоретический характер и включает научные основы защищенного документооборота, рассмотрение организационных и технических каналов несанкционированного доступа к документам, функциональные возможности и эффективность различных способов и систем обработки, движения и хранения документов. Во втором разделе освещаются технологические стадии, процедуры и операции защиты и обработки документов. Третий раздел предполагает усвоение студентами технологии защиты конфиденциальных документов в архиве. В четвертом разделе дается авторская методика проектирования локальных и комплексных направлений совершенствования защищенного документооборота.**

**Предметом изучения курса являются основы документационного обеспечения управления (ДОУ), при этом главное место занимает рассмотрение вопросов управления документацией (документационного менеджмента) и документирования деятельности работников и структурных подразделений, в том числе служб, ответственных за выполнение режимных требований.**

**Целью дисциплины является формирование навыков организации эффективной системы документационного обеспечения управления деятельностью предприятия (организации, учреждения).**



**В курсе изучаются и анализируются законодательные и нормативно-правовые акты по документационному обеспечению управления, рассматриваются вопросы организационного регулирования документационных процессов, теории и практики современной технологии документооборота, этапы и стадии работы с документами (включая получение, создание, обработку, отправку, хранение и уничтожение документов, экспертизу их ценности, формирование дел и передачу их в архивы), взаимодействие традиционной и электронной систем делопроизводства.**

### **Дисциплины по выбору студента**

#### **Б3.В.ДВ.1-1. «Экономические аспекты защиты информации»**

Дисциплина «Экономические аспекты защиты информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы, «Основы исследований информационной безопасности», «Организационно-правовое обеспечение информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные

консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 6 семестре.

**Курс содержит сведения об основных экономических понятиях и критериях определения экономической эффективности защиты информации; об основных факторах, определяющих возможную величину ущерба; о методах оценки эффективности инвестиций в защиту информации; о видах рисков; об использовании страхования в целях защиты информации.**

**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 методов и средств защиты информации, обеспечивать выбор наиболее эффективных проектов инвестиций в защиту информации.**

**В содержании курса раскрываются 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. Изучаются вопросы управления ресурсами в процессе защиты информации, а также порядок формирования бюджета службы защиты информации на предприятии.**

### **Б3.В.ДВ.1-2. «Защищенные электронные технологии банка»**

Дисциплина «Защищенные электронные технологии банка» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 6 семестре.

**Предметом изучения курса являются основы банковского бизнеса - технологии расчетной, депозитной, кредитной, бухгалтерской работы банков и пр., с применением для этого информационных технологий.**

**Целью дисциплины является формирование знаний в области использования информационных технологий для организации эффективной работы банков.**

**Содержание курса охватывает следующие темы: формы и технология безналичных расчетов в РФ, технологии межбанковских платежей, нетто-расчеты и брутто-расчеты, система ВРРВ Банка России. Корреспондентские отношения между банками (расчеты по счетам «лоро»/«ностро»), расчеты через клиринговые организации, внутрибанковские и межфилиальные расчеты, унифицированные форматы электронных банковских сообщений; организация наличного денежного оборота, дистанционное банковское обслуживание, розничные платежные системы, системы платежей по банковским картам, системы «электронных денег», «виртуальных счетов» и «виртуальных чеков»; формы и технологии международных расчетов, расчеты платежными сообщениями через систему SWIFT, расширения языка XML для передачи финансовой информации; депозитная работа в коммерческом банке, кредитная работа в коммерческом банке, операции с ценными бумагами, депозитарное обслуживание, операции с драгоценными металлами, обслуживание «металлических» счетов; управление ликвидностью коммерческого банка, управление банковскими рисками, основы бухгалтерского учета в коммерческом банке, банковский маркетинг.**

## **Б3.В.ДВ.2-1. «Эффективность защищенных информационных систем»**

Дисциплина «Эффективность защищенных информационных систем» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации», «Управление информационной безопасностью» и др.

Изучение данной дисциплины базируется на знаниях школьной программы: эффективность защищенных информационных систем.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 4 курс, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 8 семестре.

**Предмет курса - контроль состояния и эффективности защиты информации в процессе эксплуатации объектов информатизации.**

**Цель курса — формирование практических навыков проведения оценки эффективности защиты информации.**

**Содержание курса охватывает такие вопросы, как выявление уязвимостей и оценка рисков с использованием систем анализа защищенности, средства контроля защищенности (сканеры безопасности, системы обнаружения вторжений), формирование**

**системы показателей эффективности, основные методы контроля состояния и эффективности защиты информации, оценка выполнения требований нормативных документов, обоснованности принятых мер защиты информации, аттестация автоматизированных систем.**

### **Б3.В.ДВ.2-2. «Защита деловой переписки (секреты безопасности)»**

Дисциплина «Защита деловой переписки (секреты безопасности)» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации», «Управление информационной безопасностью» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 4 курс, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета с оценкой в 8 семестре.

**Предметом изучения курса являются основы документационного обеспечения управления (ДОУ), при этом главное место занимает рассмотрение вопросов управления документацией (документационного менеджмента) и документирования деятельности работников и структурных подразделений, в том числе служб, ответственных за выполнение режимных требований и организации деловой переписки.**

Целью дисциплины является формирование навыков организации эффективной системы документационного обеспечения управления деятельностью предприятия (организации, учреждения).

В курсе изучаются и анализируются законодательные и нормативно-правовые акты по документационному обеспечению управления, рассматриваются вопросы организационного регулирования документационных процессов, теории и практики современной технологии документооборота, этапы и стадии работы с документами (включая получение, создание, обработку, отправку, хранение и уничтожение документов, экспертизу их ценности, формирование дел и передачу их в архивы), взаимодействие традиционной и электронной систем делопроизводства.

### **Б3.В.ДВ.3-1. «Введение в профессию»**

Дисциплина «Введение в профессию» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: введение в профессию.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ПК-10: способностью администрировать подсистемы информационной безопасности объекта;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 1 курсе, в 1 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

Целью изучения дисциплины является ознакомление и закрепление базовых положений по обеспечению информационной безопасности на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Дисциплина базируется на одновременно изучаемых дисциплинах: “Математика”, “Физика”, ”Основы права “, “Основы информатики “ и компетенциях ОК - 3, -5, -8, -9, -11, -12, ПК – 2, -6, -8, -11, -19, -20, -24.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин профессионального цикла (базовой и вариативной частей) и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ДВ.3-2. «Введение в информационную безопасность (для сотрудников предприятия)»**

Дисциплина «Введение в информационную безопасность (для сотрудников предприятия)» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: введение в информационную безопасность (для сотрудников предприятия).

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ПК-10: способностью администрировать подсистемы информационной безопасности объекта;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 1 курсе, в 1 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 1 семестре.

Целью изучения дисциплины является формирование у студентов первичных знаний и элементарных навыков по профессии бакалавра информационной безопасности и основ ее освоения в высшей школы, тематике и особенностях предстоящего обучения.

Дисциплина базируется на одновременно изучаемых дисциплинах: “Математика”, “Физика”, ”Правоведение “, “Информатика“, «Основы

информационной безопасности» и следующих компетенциях: ОК - 3, -5, -8, -9, -11, -12, ПК – 2, -6, -8, -11, -17 -19, -20, -24.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении всех дисциплин профессионального цикла (базовой и вариативной частей) и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ДВ.4-1. «Разработка политики информационной безопасности в организациях»**

Дисциплина «Разработка политики информационной безопасности в организациях» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации», и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

**Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления**



**информационной безопасностью (СУИБ) для различных предприятий и организаций.**

**Целью курса является формирование умения планировать и обосновывать мероприятия по разработке и внедрению СУИБ, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности СУИБ.**

**Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению политики безопасности предприятия (организации), в том числе: инициирование проекта, определение области действия и политики**

**безопасности, проведение анализа предприятия (организации), оценку рисков и планирование обработки рисков, проектирование СУИБ, планирование внутренних аудитов и мониторинга показателей эффективности информационной безопасности.**

### **Б3.В.ДВ.4-2. «Разработка политики информационной безопасности в Интернет - системах»**

Дисциплина «Разработка политики информационной безопасности в Интернет-системах» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Криптографические методы защиты информации», «Техническая защита информации», и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных

занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

**Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной безопасностью (СУИБ) для различных предприятий и организаций.**

**Целью курса является формирование умения планировать и обосновывать мероприятия по разработке и внедрению СУИБ, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности СУИБ.**

**Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению политики безопасности предприятия (организации), в том числе: инициирование проекта, определение области действия и политики безопасности, проведение анализа предприятия (организации), оценку рисков и планирование обработки рисков, проектирование СУИБ, планирование внутренних аудитов и мониторинга показателей эффективности информационной безопасности.**

### **БЗ.В.ДВ.5-1. «Управление рисками в области защиты информации»**

Дисциплина «Управление рисками в области защиты информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Организационно-правовое обеспечение информационной», «Основы исследований информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной самостоятельной деятельности в условиях информационного противоборства;

ПК-6: способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 4 курсе, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 8 семестре.

**Курс представляет собой изложение важной области современного менеджмента, связанной с планированием и организацией мероприятий по обеспечению информационной безопасности, направленных на минимизацию неблагоприятного влияния рисков, вызванных случайными событиями.**

**Целью курса является формирование знаний о методах анализа риска, умении учитывать риски при управлении информационными бизнес-процессами, сопоставлять риски разной природы, оценивать меры риска, предлагать способы и средства по их минимизации.**

**Структура курса предполагает рассмотрение основных понятий, связанных с управлением информационными рисками, концепции управления рисками, методами анализа и снижения рисков, а также методикой принятия решений в условиях рисков.**

### **Б3.В.ДВ.5-2. «Защита информации от несанкционированного доступа»**

Дисциплина «Защита информации от несанкционированного доступа» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется ранее изученных дисциплинах: «Техническая защита информации», «криптографические методы защиты информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-5: способностью к кооперации с коллегами, работе в коллективе;

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ПК-6: способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

Общая трудоемкость освоения дисциплины 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 4 курсе, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 8 семестре.

**В курсе рассматриваются теоретические и прикладные аспекты проблемы защиты программного обеспечения от деструктивных воздействий. Особое внимание уделено моделям и методам создания доказуемо защищенных программ для применения в компьютерных системах с высоким оценочным уровнем доверия.**

**Целью курса является приобретение знаний о современных методах защиты программ от средств деструктивного типа, а также методов защиты программ от несанкционированного исследования, копирования, распространения и использования.**

**Содержание курса охватывает методологические основы проблемы защиты программ для различных объектов автоматизации, моделей угроз и принципов обеспечения безопасности. Рассматриваются методы обеспечения безопасности программ на этапе их разработки и испытаний, создания программного обеспечения, позволяющего игнорировать или автоматически устранять программные дефекты. Изучаются вопросы обеспечения технологической безопасности программ, реализуемые на этапах тестирования и испытания программных комплексов и методы защиты программ от генерации программных закладок инструментальными средствами, а также методы обеспечения эксплуатационной безопасности (обеспечение**

**целостности и достоверности программного кода, защите от несанкционированного исследования, копирования и распространения).**

### **Б3.В.ДВ.6-1. «Организации защиты персональных данных на предприятиях»**

Дисциплина «Организация защиты персональных данных на предприятиях» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: организация защиты персональных данных на предприятиях.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

Общая трудоемкость освоения дисциплины 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 7 семестре.

**Содержание дисциплины охватывает круг вопросов, связанных с организацией обработки персональных данных, в соответствии с требованиями российского законодательства, применительно к различным категориям исполнителей на предприятии (от руководителей предприятий и структурных подразделений до непосредственно отвечающих за защиту информации и работающих с персональными данными). Анализируются изменения российского законодательства в части персональных данных, последствия внесения этих изменений для деятельности операторов, способы минимизации**

рисков, связанных с обработкой персональных данных и затрат на их защиту.

Цель курса - 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.

Структура курса предполагает рассмотрение теоретических и практических аспектов в работе с персональными данными на предприятии, а также разбор на практических примерах действий операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношениях, связанных с передачей и представлением персональных данных третьим лицам, в том числе органам государственной власти.

### **БЗ.В.ДВ.6-2. «Правовая охрана результатов интеллектуальной деятельности»**

Дисциплина «Правовая охрана результатов интеллектуальной деятельности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-6: способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

Общая трудоемкость освоения дисциплины 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 4 курсе, в 7 семестре,

продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена в 7 семестре.

**В курсе раскрываются базовые понятия и определения в сфере интеллектуальной собственности, т.е. различных результатов интеллектуальной деятельности и средств индивидуализации производителей товаров и услуг, в том числе понятия интеллектуальных прав, исключительного права и личных прав авторов, защиты исключительных и личных прав и ответственности за нарушение указанных прав. Рассматриваются особенности различных институтов интеллектуальной собственности, включая авторское право и смежные права, патентное право, права на средства индивидуализации, права на секреты производства. Даются механизмы правовой охраны, используемые в глобальных сетях и в отношениях между партнерами из разных государств на основе многосторонних конвенций в сфере интеллектуальной собственности.**

**Целью курса является формирование представлений об эффективном использовании норм законодательства, регламентирующих механизмы охраны исключительных прав и защиты прав как на отдельные результаты интеллектуальной деятельности (изобретения, промышленные образцы, полезные модели, произведения авторского права и объекты смежных прав), так и на приравненные к ним средства индивидуализации производителей товаров и услуг.**

**Содержание курса охватывает круг вопросов, связанных с изучением законодательных и иных нормативно-правовых актов, регламентирующих деятельность в сфере охраны прав на результаты интеллектуальной деятельности; с правовым регулированием взаимоотношений работодателей и работников в части результатов интеллектуальной деятельности; с регулированием гражданско-правовых отношений, возникающих в связи с использованием прав на результаты интеллектуальной деятельности; с защитой прав правообладателей результатов интеллектуальной деятельности и средств индивидуализации.**

### **Б3.В.ДВ.7-1. «Защита профессиональной тайны в различных сферах деятельности»**

Дисциплина «Защита профессиональной тайны в различных сферах деятельности» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Организационно-правовое обеспечение информационной безопасности», «Введение в профессию» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестр, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

Содержание дисциплины охватывает круг вопросов, связанных с нормативно-правовыми аспектами защиты профессиональной тайны. Общая проблема защиты профессиональной деятельности имеет две стороны. Приводятся сведения об оформлении заявочных материалов на изобретение, полезную модель и промышленный образец. Подробно рассматриваются вопросы правовой защиты объектов интеллектуальной промышленной собственности (патентное право).

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: информационная безопасность предприятия (организации), управление информационной безопасностью.



### **Б3.В.ДВ.7-2. «Информационная безопасность операционных систем и баз данных»**

Дисциплина «Информационная безопасность операционных систем и баз данных» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Информатика», «Математика» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестр, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

Курс охватывает круг вопросов, связанных с проблематикой разработки и развития методов обеспечения информационной безопасности операционных систем и баз данных, а также выбором эффективных механизмов для их реализации.

**Цель курса - формирование базовых знаний в области обеспечения информационной безопасности операционных систем и баз данных; навыков организации работы по проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.**

**Содержание курса включает рассмотрение понятийного базиса в области обеспечения информационной безопасности операционных систем и баз данных; 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, антивирусная защита, обнаружение вторжений, межсетевое экранирование, виртуализация как механизм защиты информации в сетях; элементы криптографической защиты; основы безопасности программного обеспечения; вопросы организации обеспечения информационной безопасности систем: нормативная база, структура и принципы построения системы обеспечения информационной безопасности, рубежи защиты систем и связанные с ними задачи, виды и этапы обеспечения информационной безопасности, элементы управления информационной безопасностью систем.**

### **БЗ.В.ДВ.8-1. «Аттестация объектов информатизации»**

Дисциплина «Аттестация объектов информатизации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности», «Инженерно-техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной самостоятельной деятельности в условиях информационного противоборства;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и

нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 4 курсе, в 8 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 8 семестре.

**В курсе освещены вопросы организации и проведения аттестации защищаемого объекта информатизации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности 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.**

**В курсе рассматриваются функции органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации. Изучается порядок проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформление и регистрация аттестата соответствия.**

### **БЗ.В.ДВ.8-2. «Информационно-психологическая безопасность»**

Дисциплина «Информационно-психологическая безопасность» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности», «Инженерно-техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-7: способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства;

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

ПСК-4: способен организовать контроль защищенности объектов в соответствии с нормативными документами.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц, 72 часа. Преподавание дисциплины ведется на 4 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета в 6 семестре.

Целями изучения дисциплины является: обучение студентов принципам и средствам обеспечения информационной безопасности личности (сотрудников), коллективов (организационных структур предприятий) и в целом общества (предприятий); получение студентами фундаментальных основ по формированию научного мировоззрения, развитию системного мышления и интеграции полученных ранее знаний по обеспечению информационной безопасности.

Основные задачи дисциплины – дать основные знания, умения и навыки по вопросам обеспечения информационной безопасности личности (сотрудника), коллектива сотрудников (отделов, служб) и, в целом, всего коллектива предприятия как общества.

Дисциплина базируется на одновременно изучаемых дисциплинах: “Математика”, “Физика”, ”Правоведение “, “Информатика “, «Основы информационной безопасности» и следующих компетенциях: ОК-1, -2, -3, -7; ПК -2, -3, -19.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении всех дисциплин

профессионального цикла (базовой и вариативной частей) и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ДВ.9-1. «Организация работы с персоналом, допущенным к конфиденциальной информации»**

Дисциплина «Организация работы с персоналом, допущенным к конфиденциальной информации» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: организация работы с персоналом, допущенным к конфиденциальной информации.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

ПСК-1: способен проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников угроз, их вероятных целей и тактики;

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета 6 семестре.

**Курс рассматривает теорию и практику работы с персоналом, допущенным к конфиденциальной информации, как одно из основных**

**направлений в деятельности организации и ее структурных подразделений.**

**Целью курса является изучение основ организации работы с персоналом, допущенным к конфиденциальной информации (на всех этапах от подбора кандидатов на должности до прекращения трудовых отношений).**

**Содержание курса включает рассмотрение принципов подбора, расстановки, планирования, распределения, адаптации и мотивирования персонала, его обучения, инструктажа, стажировки, проверки специальных знаний. Особое внимание уделяется организации текущей работы, взаимодействия администрации и работников, а также регламентации отношений с правоохранительными органами.**

### **БЗ.В.ДВ.9-2. «Правонарушения в информационной сфере»**

Дисциплина «Правонарушения в информационной сфере» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы: правонарушения в информационной сфере.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-11: способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные

консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета 6 семестре.

**Курс освещает вопросы правонарушений в информационной сфере и применения мер юридической ответственности за них.**

**Цель курса - формирование знаний в области правовых аспектов информационной безопасности и, прежде всего, об основных нормативных актах, действующих в информационной сфере; формирование навыков правомерного поведения, выявления и предотвращения информационных правонарушений и защиты от них.**

**Содержание курса объединяет ряд логически связанных разделов, включающих общие теоретические вопросы юридической ответственности и изучение основных видов правонарушений в информационной сфере, ответственности за их совершение и методов противодействия им. Рассматриваются: право на доступ к информации и ответственность его нарушения; нарушения при использовании информации с ограниченным доступом; посягательства на честь, достоинство и деловую репутацию граждан и юридических лиц; незаконное распространение информации; ответственность за нарушение интеллектуальных прав; особенности применения мер юридической ответственности за правонарушения в глобальных компьютерных сетях.**

### **Б3.В.ДВ.10-1. «Социотехносферная безопасность объектов информационной защиты»**

Дисциплина «Социотехносферная безопасность объектов информационной защиты» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности», «Инженерно-техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена 6 семестре.

Целями изучения дисциплины являются: Дать студентам базовые знания по основам обеспечения социотехносферной безопасности ключевых объектов информационной защиты на предприятиях, организациях и учреждениях в современных условиях; Выработать и закрепить у студентов первичные умения и навыки по организации и реализации технологий социотехносферной безопасности объектов информационной защиты на предприятиях (организациях и учреждениях) с различными формами собственности с учетом современных подходов обеспечения информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Организационное и правовое обеспечение информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности», «Техническая защита информации» и компетенциях: ОК-1, -7, ПК-1,-2,-3,-19 и ПСК-1,2.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин профессионального цикла «Информационная безопасность автоматизированных систем», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Информационная безопасность предприятия» и выполнении выпускной квалификационной работы бакалавра.

### **Б3.В.ДВ.10-2. «Защита общества от информации, запрещенной к распространению»**

Дисциплина «Защита общества от информации, запрещенной к распространению» относится к базовой части профессионального цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.



Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Основы информационной безопасности», «Организационно-правовое обеспечение информационной безопасности», «Инженерно-техническая защита информации» и др.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-9: способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 3 курсе, в 6 семестре, продолжительностью 18 недель и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме экзамена 6 семестре.

**Курс содержит основные сведения, касающиеся организации и технологии организационно-правовой защиты общества от информации, законодательно запрещенной для создания и последующего распространения, в том числе информации, возбуждающей социальную, расовую, национальную и религиозную ненависть и вражду, призывающей к войне или пропагандирующей войну, а также посягающей на честь и достоинство гражданина, на деловую репутацию физического или юридического лица.**

**Цель курса - сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность и научить способам организационно-правовой защиты личности и общества от информации, законодательно запрещенной для создания и последующего распространения.**

**В структуре курса подробно рассматриваются способы организационно-правовой защиты от создания и распространения ненадлежащей рекламы и меры ответственности за нарушение российского рекламного законодательства. Отдельный раздел**

дисциплины предусматривает изучение общих принципов, которые могут быть использованы для обеспечения организационно-правовой и технической защиты пользователей сети Интернет от законодательно запрещенной к распространению информации, а также изучение концепции государственной политики в области защиты детей от информации, причиняющей вред их здоровью и развитию.

## **ФИЗИЧЕСКАЯ КУЛЬТУРА**

### **Б4. «Физическая культура»**

Дисциплина «Физическая культура» относится к базовой части физической культуры цикла основной образовательной программы подготовки студентов по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на знаниях школьной программы: физическая культура.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-12: способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;

ОК-13: способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

Целью изучения дисциплины является:

формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности.

Дисциплина базируется на знаниях, умениях и навыках, полученных на уроках физической культуры в средних образовательных учреждениях.

Полученные студентами знания способствуют усвоению таких курсов как История, Концепция современного естествознания, Безопасность жизнедеятельности.

Целью изучения дисциплины является: формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей профессиональной деятельности.

Дисциплина базируется на знаниях, умениях и навыках, полученных на уроках физической культуры в средних образовательных учреждениях.

Полученные студентами знания способствуют усвоению таких курсов как История, Концепция современного естествознания, Безопасность жизнедеятельности.

Общая трудоемкость освоения дисциплины составляет 11 зачетных единицы 400 часов. Преподавание дисциплины ведется на 1,2,3 курсах продолжительность семестра 18 недель. Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, промежуточная аттестация в форме зачета 1-6 семестре.

Критерием успешности освоения учебного материала является экспертная оценка преподавателя, учитывающая регулярность посещения учебных занятий, знаний теоретического раздела программы, выполнение установленных тестов общей физической и спортивно-технической подготовки.

Обязательные тесты проводятся в начале учебного года как контрольные, характеризующие уровень физической подготовленности первокурсника при поступлении в вуз и физическую активность студента в каникулярное время, и в конце учебного года – как определяющие сдвиг в уровне физической подготовленности за прошедший учебный год.