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

Блок 1. Дисциплины (модули)

Обязательная часть

Б1.О.01 «Философия»

Дисциплина «Философия» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: отдельных разделах «История России», «Основы права» и компетенциях: УК-1, УК-5, ПК-1.

Дисциплина направлена на формирование следующих компетенций:
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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 4 зачетные единицы, 144 часа. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной и в 4 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 2 семестре для очной и в 4 семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы управления информационной безопасностью», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»,

прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.02 «История России»

Дисциплина «История России» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы российской государственности» и компетенциях УК-5.

Дисциплина направлена на формирование следующих компетенций:
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;

Содержание дисциплины включает в себя круг вопросов, направленных на формирование целостного представления об историческом пути России в контексте общемирового исторического развития; развитие патриотического сознания студенчества.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 1 и 2 курсе во 2 и 3 семестре для очной и на 1 и 2 курсе во 2 и 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы, зачета с оценкой во 2 семестре для очной и очно-зачетной формы обучения и экзамена в 3 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: отдельные разделы дисциплины «Философия», «Организация системы обеспечения информационной безопасности (служба ИБ)», «История защиты информации в РФ», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.03 Основы российской государственности

Дисциплина «Основы российской государственности» относится к дисциплинам по выбору части, формируемой участниками образовательных

отношений, основной образовательной программы подготовки бакалавров по направлению подготовки 10.03.01 «Информационная безопасность».

Дисциплина базируется на уроках обществознания в среднеобразовательных учебных заведениях, и опирается на коммуникативные компетенции, приобретённые в средней общеобразовательной школе.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;

Содержание дисциплины охватывает круг вопросов, связанных с изучением исторических, географических, институциональных оснований формирования российской цивилизации, помогает обучающимся расставить мировоззренческие акценты, сформировать чувство гражданственности и принадлежности к российскому обществу. Также содержательная часть данного курса способствует созданию духовно-нравственного и культурного фундамента развитой и цельной личности, осознающей особенности исторического пути российского государства и самобытность его политической организации.

Общая трудоемкость дисциплины для студентов очной формы обучения составляет 2 зачетных единицы, 72 часа.

Преподавание дисциплины ведется на 1 курсе во 1 семестре при очной форме обучения и на втором курсе во 2 семестре для очно-заочной формы обучения, 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 и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре при очной и во 2 семестре очно-заочной форме обучения.

Основные положения и знания, полученные при освоении дисциплины должны быть использованы при изучении последующих дисциплин: «Основы управленческой деятельности», «Основы права», «Введение в профессию» и выполнении выпускной квалификационной работы бакалавра.

Б1.О.04 «Иностранный язык» (английский, французский, немецкий языки)

Дисциплина «Иностранный язык» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой иностранного языка.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (ых) языке(ах);
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

Предметом учебного курса является иностранный язык (английский, французский, 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.

Общая трудоемкость освоения дисциплины составляет 10 зачетных единиц, 360 часов. Преподавание дисциплины ведется на 1 и 2 курсах в 1-4 семестрах для очной и очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 1 и 3 семестрах и в форме контрольной работы и экзамена во 2 и 4 семестрах в форме контрольной работы и экзамена для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Моделирование процессов и систем защиты информации», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.05 «Безопасность жизнедеятельности»

Дисциплина «Безопасность жизнедеятельности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления качеством и стандартизации.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;
УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 1 семестре для очной и во 2 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 1 семестре для очной и во 2 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Физическая

защита информационных объектов», «Конфиденциальное делопроизводство и защищенный электронный документооборот», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.6 «Физическая культура»

Дисциплина «Физическая культура» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-7. Способен поддерживать должный уровень 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.

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и в 2 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и зачета во 2 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Элективные курсы по физической культуре и спорту», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.07 «Русский язык и культура речи»

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

Дисциплина реализуется кафедрой иностранных языков.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном (ых) языке(ах);
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

Курс русского языка и 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 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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре

для очной формы обучения и очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения и в форме контрольной работы и зачета в 1 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Основы управления информационной безопасностью», «Основы информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.8 «Основы управленческой деятельности»

Дисциплина «Основы управленческой деятельности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и на 1 курсе во 2 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной и во 2 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «История (история России, всеобщая история)», «Основы управления информационной безопасностью», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.9 «Документоведение»

Дисциплина «Документоведение» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и

поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

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.

Общая трудоемкость освоения дисциплины 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и в 1 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной формы обучения и в 1 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация системы обеспечения информационной безопасности (служба ИБ)», «Конфиденциальное делопроизводство и защищенный электронный документооборот», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.10 «Экономика предприятия и организация производства»

Дисциплина «Экономика предприятия и организация производств» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой экономики.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;

Содержание дисциплины охватывает круг вопросов, связанных с изучением закономерностей экономической жизни общества, способов решения базовых экономических проблем в рамках экономических систем различных типов; основных микро- и макроэкономических подходов и особенностей их применения в России на современном этапе; закономерностей и принципов поведения экономических агентов в современной экономике; основных понятий, категорий и методов экономической теории; экономических законов и основных особенностей ведущих школ и направлений экономической науки.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единицы, 216 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре и на 2 курсе в 3 семестре для очной формы обучения и в 1 семестре и 2 семестре и на 2 курсе в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре и в форме контрольной работы и контрольной работы и экзамена в 3 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Математическая логика и теория алгоритмов», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.О.11 Группа учебных дисциплин (модулей) «Математические основы обеспечения информационной безопасности»

Б1.О.11.01 «Линейная алгебра и аналитическая геометрия»

Дисциплина «Линейная алгебра и аналитическая геометрия» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы математического анализа и моделирования в профессиональной деятельности.

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Преподавание дисциплины ведется на 1-ом курсе, в 1-ом, семестре, продолжительностью 16 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 контрольной работы и экзамена в 1-ом семестре для очной формы обучения и в 1-ом семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.02 «Математический анализ»

Дисциплина «Математический анализ» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы математического анализа и моделирования в профессиональной деятельности.

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 1-ом курсе, во 2-ом семестре, продолжительностью 16 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 контрольной работы и экзамена во 2-ом семестре для очной формы обучения и во 2-ом семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.03 «Теория графов»

Дисциплина «Теория графов» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

Целью изучения дисциплины является: формирование способности к восприятию, обобщению и анализу информации; освоение необходимого математического аппарата, применяемого при решении различных профессиональных задач; формирование готовности применять методы математического анализа и моделирования в профессиональной деятельности. 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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2-ом курсе в 3 семестре, продолжительностью 16 недель для очной и на 2-ом курсе в 4 семестре, продолжительностью 16 недель для очно-заочной 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 контрольной работы и экзамена в 3 семестре для очной формы обучения и в форме контрольной работы и экзамена в 4 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Математическая логика и теория алгоритмов», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.04 «Теория информации»

Дисциплина «Теория информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», отдельные разделы «Экономика предприятия и организация производства», «Документоведение»,«Математический анализ» и компетенциях: УК-3,7,8,9, ОПК-2,3,8,10,12,13.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной формы обучения и в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в

форме контрольной работы и зачета с оценкой в 3 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Физическая защита информационных объектов», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.05 «Теория вероятностей и математическая статистика»

Дисциплина «Теория вероятностей и математическая статистика» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика» и компетенциях: ОПК-2,3,7,9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;

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, конт 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.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 2 курсе в 3-4 семестрах для очной формы обучения и на 2-3 курсах в 4-5 семестрах для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и в форме контрольной работы и экзамена в 4 семестре для очной формы обучения и в форме контрольной работы и зачета в 4 семестре и в форме контрольной работы и экзамена в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Экономика информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.11.06 «Дискретная математика»

Дисциплина «Дискретная математика» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации» и компетенциях: ОПК-2,3,11 .

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения и в форме контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Экономика информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.О.12 Группа учебных дисциплин (модулей) «Физико-технические основы обеспечения информационной безопасности»

Б1.О.12.01 «Физика»

Дисциплина «Физика» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика», «Экономика предприятия и организация производства» и компетенциях: ОПК-2,3,7,9,12, УК-9.

Дисциплина направлена на формирование следующих компетенций:

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов;

Содержание дисциплины охватывает круг вопросов, связанных с классическими разделами физики: механика, молекулярная физики 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.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов. Преподавание дисциплины ведется на 1-2 курсах в 2-3 семестрах для очной формы обучения и 2-3 семестрах очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре и в форме контрольной работы и экзамена в 3 семестре для очной формы обучения и зачёта во 2 семестре и экзамена во 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Электротехника», «Электроника и схемотехника», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.12.02 «Электротехника»

Дисциплина «Электротехника» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Физика», «Математический анализ», «Теория вероятностей и математическая статистика» и компетенциях: ОПК-2,3,4,11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

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, имеющихся 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.

Общая трудоемкость освоения дисциплины 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения и для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Радиоэлектронные системы и средства как объекты информационной безопасности», «Основы радиоэлектронной разведки (РЭР)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.12.03 «Электроника и схемотехника»

Дисциплина «Электроника и схемотехника» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Электротехника» и компетенциях: ОПК-2,3, 4,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения и в форме контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Радиоэлектронные системы и средства как объекты информационной безопасности», «Основы радиоэлектронной разведки (РЭР)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.О.13 Группа учебных дисциплин (модулей) «Информационные технологии»

Б1.О.13.01 «Информатика»

Дисциплина «Информатика» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и в 1 семестре очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 1 семестре для очной и в форме контрольной работы и экзамена в 1 семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Моделирование процессов и систем защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.02 «Языки программирования»

Дисциплина «Языки программирования» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации» и компетенцияхОПК-2,3, 11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и на 3 курсе в 5 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 4 семестре для очной формы обучения контрольной работы и экзамена в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Моделирование процессов и систем защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.03 «Технологии и методы программирования»

Дисциплина «Технологии и методы программирования» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования» и компетенциях: ОПК-2,3,7,9,11.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и в форме контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-

аппаратные средства защиты информации», «Моделирование процессов и систем защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.04 «Информационные технологии»

Дисциплина «Информационные технологии» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования», «Аппаратные средства вычислительной техники», «Сети и системы передачи информации» и компетенциях: ОПК-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов:

лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения и контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Программно-аппаратные средства защиты информации», «Моделирование процессов и систем защиты информации», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.05 «Аппаратные средства вычислительной техники»

Дисциплина «Аппаратные средства вычислительной техники» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования» и компетенциях: ОПК-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-2. Способен применять информационно – коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы обучения и контрольной работы и экзамена в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Программно-аппаратные средства защиты информации», «Моделирование процессов и систем защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Криптографические методы защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.13.06 «Сети и системы передачи информации»

Дисциплина «Сети и системы передачи информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория вероятностей и математическая статистика», «Теория информации», «Языки программирования», «Технологии и методы программирования», «Аппаратные средства вычислительной техники» и компетенциях: ОПК-2,3,7,9,11,.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

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 TCPДР, архитектуру и средства взаимодействия процессов в сетях, основные принципы построения и современные тенденции развития сетей. Рассматривается архитектура и топологии построения современных ЛВС, технологии Ethernet (FastEthemet, GigabitEthemet), 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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения 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: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы обучения и контрольной работы и экзамена в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Криптографические методы защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок Б1.О.14 Группа учебных дисциплин (модулей) «Методы и средства обеспечения информационной безопасности»

Б1.О.14.01 «Основы информационной безопасности»

Дисциплина «Основы информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности» и компетенциях: УК-1,2,5,10; ОПК-7; ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часа. Преподавание дисциплины ведется на 1-2 курсе в 2-3 семестрах для очной формы обучения и в 2-3 семестрах очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета во 2 семестре и контрольной работы и экзамена в 3 семестре для очной формы обучения и в форме контрольной работы во 2 семестре и зачета с оценкой в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы управления информационной безопасностью», «Организация защиты персональных данных на предприятии», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.02 «Организационное и правовое обеспечение информационной безопасности»

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности», «Основы информационной безопасности» и компетенциях: ОПК-1,6,7,8; УК-1,2,5,10; ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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 внутри объектового режимов, организационные требования к режимным помещениям, организацию совещаний (переговоров), издательской, рекламно-выставочной деятельности, проведение внутренних расследований по конфиденциальным вопросам

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 часов. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной формы обучения и на 3 курсе в 5 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 4 семестре и курсовой работы для очной формы обучения и экзамена в 5 семестре и курсовой работы для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины «Криптографические методы защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Лицензирование и сертификация в области защиты информации», являются базовыми для изучения всех последующих дисциплин, прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.03 «Основы управления информационной безопасностью»

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Основы информационной безопасности», «Математический анализ», «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот» и компетенциях:УК-1; ОПК-3; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

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).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольная работа и зачета в 6 семестре для очной формы обучения и в форме контрольной работы и зачета в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Эффективность защищенных информационных систем», «Социотехносферная безопасность объектов информационной защиты», «Правовая охрана результатов интеллектуальной деятельности», «Разработка политики информационной безопасности в Интернет-системах», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.04 «Защита информации от утечки по техническим каналам»

Дисциплина «Защита информации от утечек по техническим каналам» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности», «Основы информационной

безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОПК-1,5,6,7,8,9, УК-2,5,10 ПК-1,2,3.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (решения задач и лабораторные работы), курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 6 семестре и курсовой работы для очной формы обучения и экзамена в 7 семестре и курсовой работы для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.05 «Методы и средства криптографической защиты информации»

Дисциплина «Криптографические методы защиты информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью» и компетенциях: УК-1; ОПК-1,2,3,5,6,10.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 7 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Комплексное

обеспечение защиты информации объекта информатизации (предприятия)», «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.06 «Программно-аппаратные средства защиты информации»

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью», «Методы и средства криптографической защиты информации» и компетенциях: УК-1; ОПК-2,3,5,7,9,10.

Дисциплина направлена на формирование следующих компетенций:

ОПК-6. Способен при решении задач профессиональной деятельности организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме экзамена в 7 семестре и курсовой работы для очной формы обучения и экзамена в 8 семестре и курсовой работы для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.14.07 «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации (предприятия)» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью», «Криптографические методы защиты информации» и компетенциях: УК-1; ОПК-2,3,5,7,9,10.

Дисциплина направлена на формирование следующих компетенций:

ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем и средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

Целями изучения дисциплины являются: Дать студентам знания по организации целесообразных мероприятий по защите информации на предприятиях (организациях и учреждений) 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 учреждений) с различными формами собственности с учетом современных международных и отечественных стандартов информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 8 зачетных единиц, 288 часов. Преподавание дисциплины ведется на 4 курсе в 7-8 семестрах для очной формы обучения и в 8-9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, курсовая работа, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 7 семестре и в форме экзамена в 8 семестре и курсовой работы для очной формы обучения и в форме контрольной работы и зачета в 8 семестре и экзамена в 9 семестре и курсовой работы для очно-заочной формы обучения.

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

Блок Б1.О.15 Дисциплины (модули) профиля: «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Б1.О.15.01 «Математическая логика и теория алгоритмов»

Дисциплина «Математическая логика и теория алгоритмов» относится к обязательной части основной профессиональной образовательной программы

подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика», «Теория информации» и компетенциях: ОПК-2,3,7,9.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ОПК-3. Способен использовать совокупность необходимых математических методов для решения задач профессиональной деятельности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе 4 семестре для очной и на 3 курсе в 5 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной и в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.02 «Информационные процессы и системы как объекты информационной безопасности»

Дисциплина «Информационные процессы и системы как объекты информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Информатика», «Языки программирования» и компетенциях: УК-1; ОПК-3,7.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единиц, 144 часов. Преподавание дисциплины ведется на 2 курсе в 3-4 семестрах для очной формы обучения и на 3 курсе в 5-6 семестрах для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и в форме контрольной работы и экзамена в 4 семестре для очной формы обучения и контрольной работы и зачета в 5 семестре и контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», «Информационная безопасность автоматизированных систем», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.03 «Конфиденциальное делопроизводство и защищенный электронный документооборот»

Дисциплина «Конфиденциальное делопроизводство и защищенный электронный документооборот» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

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.

Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением процесса организации электронного документооборота на предприятиях на примере системы «ДЕЛО», разработанной компанией «Электронные Офисные Системы» (ЭОС), изучением теоретических, методологических и практических проблем, охватывающих обеспечение автоматизации процессов делопроизводства и ведение полностью электронного документооборота на объекте информатизации.

Цель курса - формирование представления об электронном документе как новой составляющей в правовых отношениях. Выявление основных особенностей «электронного документа», базовых принципов взаимодействия электронного и аналогового «миров».

Тематика курса объединена в два логически связанных раздела, имеющих практический характер применения. Первый посвящен изучению архитектуры, особенности работы систем электронного документооборота и рассмотрению функциональных возможностей системы электронного делопроизводства «ДЕЛО». Второй - основным опциям системы электронного

делопроизводства «ДЕЛО» и организации электронного документооборота, направленного на автоматизированную обработку конфиденциальных документов.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.04 «Нормативные акты и стандарты по информационной безопасности»

Дисциплина «Нормативные акты и стандарты по информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 3 курсе в 6 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.05 «Организация системы обеспечения

информационной безопасности (служба ИБ)»

Дисциплина «Организация системы обеспечения информационной безопасности (служба ИБ)» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: УК-1; ОПК-1,3,5,6,8,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

Цели преподавания дисциплины:

1) подготовить специалистов, владеющих знаниями в области организационных и правовых основ обеспечения информационной безопасности (ИБ) и организации режима секретности на объектах и системах различного профиля и организационной структуры;

2) дать основные сведения о нетехнических методиках обеспечения защиты информации, составляющей государственную и коммерческую тайну, конфиденциальной информации, а также о методиках противодействия промышленному шпионажу.

Задачами изучения дисциплины являются:

1) усвоение организационных основ построения систем защиты информации и организации работ по обеспечению ИБ на объектах информатизации (ОИ), основных подходов к комплексной оценке безопасности информации на ОИ;

2) знакомство с основными положениями государственной системы защиты информации и правового обеспечения ИБ в РФ;

3) знакомство с видами и типами компьютерных преступлений и способами противодействия различным видам атак;

4) усвоение методик построения систем организационной защиты объектов информатизации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов:

лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачет с оценкой в 7 семестре для очной формы обучения и контрольной работы и зачет с оценкой в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», отдельные разделы «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.06 «Физическая защита информационных объектов»

Дисциплина «Физическая защита информационных объектов» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ОПК-1,5,6,8,10; ДОПК-1,2,4.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-3. Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

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.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность операционных систем и баз данных», «Защита общества от информации, запрещенной к распространению», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.15.07 «Информационно-аналитическая деятельность по обеспечению комплексной безопасности»

Дисциплина «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Нормативные акты и стандарты по информационной безопасности», «Информационные процессы и системы как объекты информационной безопасности», «Информационные технологии» и компетенциях: ОПК-1,5,6,7,8,9,10; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;

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).

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

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

Б1.О.15.08 «Экономика информационной безопасности»

Дисциплина «Экономика информационной безопасности» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Экономика предприятия и организация производства», «Основы права», «История», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)» и компетенциях: УК-5,9; ОПК-5,10,12,13; ДОПК-1,2.

Дисциплина направлена на формирование следующих компетенций:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

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. Изучается вопросы управления ресурсами в процессе защиты информации, а также порядок формирования бюджета службы защиты информации на предприятии.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и на 5 курсе в 10 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 8 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

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

Б1.О.15.09 «Моделирование процессов и систем защиты информации»

Дисциплина «Моделирование процессов и систем защиты информации» относится к обязательной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Физическая защита информационных объектов», «Основы управления информационной безопасностью», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ДОПК-1,2,3,4; ОПК-5,10.

Дисциплина направлена на формирование следующих компетенций:

ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

Предметом изучения курса являются теоретические, методологические и практические вопросы системных исследований на основе математического моделирования процессов и систем зашиты информации в области обеспечения комплексной информационной безопасности современных объектов различного назначения, включая и финансово-кредитную сферу. В дисциплине современные методы математического моделирования рассматриваются как универсальный инструмент обоснования целесообразных мер (решений) сложнейших проблем, возникающих в ходе построения и развертывания новейших вариантов информационной безопасности.

Целью курса является формирование первичных знаний, умений и практических навыков по основам моделирования процессов и систем в области защиты информации на основе разработки компьютерного моделирования и обработки результатов вычислительных экспериментов, а также формирование представления о работе с современными инструментальными системами моделирования.

Тематика курса объединена в виде логически увязанных разделов. Первый носит общетеоретический характер и включает научные основы методов и методологии анализа и синтеза выявления и разрешения проблемных вопросов по защите информации. Во втором разделе освещаются методико-прикладные аспекты математического моделирования организации комплексного обеспечения информационной безопасности применительно к типовым предприятиям (организациям и учреждениям), включая и финансово

- кредитные структур. Рассматриваются в системном виде основные этапы и процессы построения комплексных систем защиты информации, состав обеспечивающих их компонентов, принципы и содержание управления, а также и вопросы оценки эффективности информационной безопасности.

Предметом изучения курса являются процессы и систем организации защиты информации с ориентацией на сложные информационные объекты.

Целевая направленность курса предусматривает формирование навыков математического обоснования целесообразных управленческих решений, прежде всего в ходе информационно-аналитической деятельности по защите информации.

В курсе также изучаются и анализируются существующие законодательные и нормативно-правовые документы по разработке и функционированию современных систем защиты информации в тесном взаимодействии со всеми видами обеспечения информационной безопасности.

В результате освоения дисциплины студент должен:

-знать: принципы построения аналитико-имитационных моделей информационных процессов, основные классы моделей и методы моделирования, методы формализации, алгоритмизации и реализации моделей на ЭВМ; приемы, методы, способы формализации объектов, процессов, явлений и реализации их на компьютере;

-уметь: использовать современные методы и инструментальные средства моделирования при исследовании процессов и проектировании систем защиты информации; планировать проведение имитационных экспериментов и обрабатывать их результаты;

-владеть: технологией математического и компьютерного моделирования при анализе процессов и синтезе современных систем защиты информации.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной и на 4 курсе в 7 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, лабораторные, практические занятия (лабораторные работы), самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной и 7 семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.16 Элективные курсы по физической культуре и спорту

Дисциплина «Элективные курсы по физической культуре и спорту» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-7. Способен поддерживать должный уровень 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.

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.

Общая трудоемкость освоения дисциплины составляет 9 зачетных единиц, 328 часов для очной формы обучения и 328 часов, 9 зачётных единиц для очно-заочной формы обучения. Преподавание дисциплины ведется на 1-3 курсах в 1,3-6 семестрах для очной формы обучения и во 1 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 1,3-6 семестрах для очной формы обучения и зачета во 1 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Физическая

культура», «Физическая защита информационных объектов», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.О.17 Основы военной подготовки

Дисциплина «Основы военной подготовки» относится к обязательной части основной образовательной программы подготовки бакалавров 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой социальных и гуманитарных дисциплин.

Дисциплина базируется на ранее полученных знаниях по ранее изученным дисциплинам в средней школе, и дисциплине «Безопасность жизнедеятельности» и опирается на коммуникативные компетенции, приобретённые в средней общеобразовательной школе и компетенции: УК-7; УК-8.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-7. способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;
УК-8. способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Содержание дисциплины включает в себя основные направления социально-экономического, политического и военно-технического развития Российской Федерации, особенности развития международных отношений, правовые основы прохождения военной службы, строевую подготовку, основы тактической, медицинской подготовки и другие разделы.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часа.

Преподавание дисциплины ведется на 2 курсе в третьем семестре для очной формы обучения и на 2 курсе в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и аттестация в форме зачета в 3

семестре для очной формы обучения и в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для формирования навыков в области военной подготовки, высокого патриотического сознания, возвышенного чувства верности своему Отечеству, готовности к его защите как важнейшей конституционной обязанности в отстаивании национальных интересов Российской Федерации и обеспечении ее военной безопасности перед лицом внешних и внутренних угроз.

Часть, формируемая участниками образовательных отношений

Б1.В.0.1 Дисциплины (модули) образовательной организации

Б1.В.01.01 «Основы исследований информационной безопасности»

Дисциплина «Основы исследований информационной безопасности» относится к дисциплинам по выбору основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и во 1 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 1 семестре для очной и в 1 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Управление информационной безопасностью», «Экономическая теория информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.02 «Пакеты прикладных программ»

Дисциплина «Пакеты прикладных программ» относится к дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

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 (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 1Р-телефонии (ICQ, Skype) и OCR (FineReader), системы машинного перевода (локальные и сетевые сервисы), Интернет-технологии поиска и управления коллективными информационными ресурсами, системы управления проектами.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Преподавание дисциплины ведется на 2 курсе во 3 семестре для очной формы обучения и на 2 курсе в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена во 3 семестре для очной формы обучения, контрольной работы и экзамена в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность кредитно-финансовых операций», «Защищенные электронные технологии банка», «Информационно-психологическая безопасность персонала предприятия», прохождения

практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.03 «Социально-психологические основы управленческой деятельности»

Дисциплина «Социально-психологические основы управленческой деятельности» относится к дисциплинам части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», «Профессиональные адаптации инвалидов и лиц с ОВЗ» и компетенциях: УК-6,8; ПК-1.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре для очной и на 2 курсе в 4 семестре очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре для очной и в 4 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии», «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.04 «Основы конкурентной разведки»

Дисциплина «Основы конкурентной разведки» относится к дисциплинам части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Безопасность жизнедеятельности», «Основы исследований информационной безопасности» и компетенциях: УК-2,7,8,10; ПК-3.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
ПК-4 Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ ТКС при возникновении внештатных ситуаций

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3,4 семестре для очной и на 3 курсе в 5,6 семестре очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов:

лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 3 семестре и зачета с оценкой в 4 семестре для очной и в 5,6 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные технологии в профессиональной деятельности», «Адаптированные информационные технологии», «Нормативные акты и стандарты по информационной безопасности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.05 «История защиты информации в РФ»

Дисциплина «История защиты информации в РФ» относится к дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: УК-5; ОПК-1,5,6,8,13.

Дисциплина направлена на формирование следующих компетенций:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 2 курсе в 4 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 4 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.01.06 «Информационная безопасность автоматизированных систем»

Дисциплина «Информационная безопасность автоматизированных систем» относится к дисциплинам части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот» и компетенциях:ОПК-1,5,6,8,9; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 7 семестре для очной формы обучения и контрольной работы и зачета в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: отдельные разделы «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.02 «Основы права»

Дисциплина «Основы права» относится к части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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 часов. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной формы обучения и на 1 курсе в 2 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 1 семестре для очной и контрольной работы и экзамена в 2 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Правовая охрана результатов интеллектуальной деятельности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.О3 «Безопасность информационных технологий»

Дисциплина «Безопасность информационных технологий» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов», «Информационные процессы и системы как объекты информационной безопасности» и компетенциях: ОПК-1,3,5,6,8; ДОПК-1,2,4.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 6 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность кредитно-финансовых операций», «Защищенные электронные технологии банка», «Разработка политики информационной безопасности в организациях», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.О4 «Гуманитарные аспекты (профессиональная этика) информационной безопасности»

Дисциплина «Гуманитарные аспекты (профессиональная этика) информационной безопасности» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Математическая логика и теория алгоритмов» и компетенциях:ОПК-1,3,5,6,8; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций выпускника:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Предметом изучения курса являются теоретические, методологические и практические вопросы изучения основных категорий общечеловеческой и профессиональной этике в области информационной безопасности современного информационного общества. Дисциплина построена на основе использования системного подхода разрешении сложнейших социально-гуманитарных проблем, возникающих в ходе построения и развертывания новейших вариантов обеспечения информационной безопасности различных информационных объектов и субъектов.

Целью курса является:

формирование у обучающихся представление о характере и механизме действия норм профессиональной этики специалиста по информационной безопасности;

умение оценивать профессиональную деятельность на основе существующих этико-профессиональных критериев в единстве и взаимодействии с требованиями общественной морали в процессе организации комплексного обеспечения информационной безопасности современных социотехнических систем.

Тематика курса объединена в виде логически увязанных двух разделов. Первый носит общегуманитарные аспекты информационной безопасности и включает: понятие и содержание гуманитарных аспектов информационной безопасности в современном информационном обществе; этапы развития и основные проблемы обеспечения информационной безопасности новейших информационных технологий. Во втором разделе освещаются основы профессиональной этики в области информационной безопасности. Рассматриваются: нравственные аспекты этики поведения в сети (локальной, корпоративной и Интернет – сети) и интеллектуальной собственности; преодоление цифрового неравенства в современном информационном обществе; понятие и характеристика кодексов этики профессиональных организаций и специалистов в области информационной безопасности.

Предметом изучения курса является профессиональная этика поведения организаций, специалистов и граждан современного информационного общества в области информационной безопасности. Использование этических знаний позволяет осуществлять поиск наиболее эффективных решений по обеспечению информационной безопасности.

Целевая направленность курса предусматривает формирование у студентов, профессионалов в области информационной безопасности, нравственно-мотивированной, социально-ответственной, целостной и компетентной личности, владеющей этическими знаниями, охватывающими становление и развитие нравственности и профессиональной этики в области информационной безопасности современного информационного общества.

Задачами дисциплины следует рассматривать:

-изучение истории развития морали и общечеловеческой этики, основных категорий и норм профессиональной этики в области информационной безопасности;

- формирование понятия нравственной культуры и факторов ее успешной реализации в профессиональной деятельности специалистов по информационной безопасности.

Изучаемый учебный материал базируется на анализе отечественного и международного опыта по формированию этических профессиональных кодексов, выработанных для области обеспечения информационной безопасности в современном информационном обществе.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 4/4 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины

ведется на 3 курсе в 6 семестре для очной и на 4 курсе в 7 семестре очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной и во 7 семестре очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.01 Дисциплины по выбору Блок 1В.ДВ.1

Б1.В.ДВ.01.01 «Операционные системы, среды и оболочки»

Дисциплина «Операционные системы, среды и оболочки» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория информации», «Основы управленческой деятельности», «Информатика» и компетенциях: ОПК-2,3,7,9; УК-6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 16/16 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и на 3 курсе в 5 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения и в форме контрольной работы и зачета в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Защищенные электронные технологии банка», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.01.02. «Базы данных, системы управления базами данных»

Дисциплина «Базы данных, системы управления базами данных» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Математический анализ», «Теория информации», «Основы

управленческой деятельности», «Информатика» и компетенциях: ОПК-2,3,7,9; УК-6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 16/16 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 2 курсе в 4 семестре для очной обучения и на 3 курсе в 5 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 4 семестре для очной формы обучения и в форме контрольной работы и зачета в 5 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Защищенные электронные технологии банка», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.02 Дисциплины по выбору Блок1.В.ДВ.2

Б1.В.ДВ.02.01 «Основы алгоритмизации и программирования»

Дисциплина «Основы алгоритмизации и программирования» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика» и компетенциях: ОПК-7,9.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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 рациональных 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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и на 2 курсе в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена во 2 семестре для очной формы обучения и в форме контрольной работы и экзамена в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.02.02 «Пакеты прикладных математических программ»

Дисциплина «Пакеты прикладных математических программ» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика» и компетенциях: ОПК-7,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе во 2 семестре для очной формы обучения и на 2 курсе в 3 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена во 2 семестре для очной формы обучения и в форме контрольной работы и экзамена в 3 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационные процессы и системы как объекты информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Моделирование процессов и систем защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03 Дисциплины по выбору Блок1.В.ДВ.3

Б1.В.ДВ.03.01 «Информационная безопасность кредитно-финансовых операций»

Дисциплина «Информационная безопасность кредитно-финансовых структур» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и экзамена в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения

практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б3.В.ДВ.03.02 «Защищенные электронные технологии банка»

Дисциплина «Защищенные электронные технологии банка» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и в форме контрольной работы и экзамена в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03.03 «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО "НОВО")

Дисциплина «Подготовка объекта информатизации к аттестации по требованиям безопасности информации (ООО «НОВО») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

Курс охватывает круг вопросов, связанных с проблематикой разработки и развития аттестации объектов информационной безопасности операционных систем и баз данных, а также выбором эффективных механизмов для их реализации.

Цель курса - формирование базовых знаний в области аттестации критически важных информационных объектов; навыков организации работы по аттестации проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Содержание курса включает рассмотрение понятийного базиса в области обеспечения аттестации объектов информационной безопасности; 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.

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 7 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация

защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.03.04 «Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")»

Дисциплина «Аттестация объекта информатизации по требованиям безопасности информации (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

Курс охватывает круг вопросов, связанных с проблематикой разработки и развития аттестации объектов информационной безопасности операционных систем и баз данных, а также выбором эффективных механизмов для их реализации.

Цель курса - формирование базовых знаний в области аттестации критически важных информационных объектов; навыков организации работы по аттестации проектированию и оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Содержание курса включает рассмотрение понятийного базиса в области обеспечения аттестации объектов информационной безопасности; 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.

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 8/8 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 5 семестре для очной формы обучения и контрольной работы и экзамена в 7 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04 Дисциплины по выбору Блок1.В.ДВ.4

Б1.В.ДВ.04.01 «Информационно-психологическая безопасность персонала предприятия»

Дисциплина «Информационно-психологическая безопасность персонала предприятия» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика»,

«Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.02 «Защита общества от информации, запрещенной к распространению»

Дисциплина «Защита общества от информации, запрещенной к распространению» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы),

самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и в форме контрольной работы и зачета с оценкой в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.03 «Организация защиты конфиденциальной информации от несанкционированного доступа (ООО "НОВО")

Дисциплина «Организация защиты конфиденциальной информации от несанкционированного доступа (ООО «НОВО») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Курс содержит основные сведения, касающиеся организации и технологии организационной защиты конфиденциальной информации от НСД. Обеспечивает выполнение установленных правовых норм, объединяет методы защиты, которые обеспечивают защиту информации от НСД либо самостоятельно, либо в комплексе с методами и средствами других направлений, с помощью организационных методов методы и средства всех направлений объединяются в сложную систему.

Цель курса - сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельности и научить способам в соответствии с нормативными документами предприятия осуществлять регулирование и организацию и выполнения работ.

В структуре курса подробно рассматриваются обеспечение защиты информации установленной технологией выполнения работ, исключающей утрату носителей информации и несанкционированный доступ к информации или к ее носителям, либо путем введения прямых правил, регулирующих организацию защиты информации от НСД.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и контрольной работы и зачета с оценкой в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.04.04 «Защита информации от НСД (ООО «ЦБИ»)»

Дисциплина «Защита информации от НСД (ООО «ЦБИ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Курс содержит основные сведения, касающиеся организации и технологии организационной защиты конфиденциальной информации от НСД. Обеспечивает выполнение установленных правовых норм, объединяет методы защиты, которые обеспечивают защиту информации от НСД либо самостоятельно, либо в комплексе с методами и средствами других направлений, с помощью организационных методов методы и средства всех направлений объединяются в сложную систему.

Цель курса - сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельности и научить способам в соответствии с нормативными документами предприятия осуществлять регулирование и организацию и выполнения работ.

В структуре курса подробно рассматриваются обеспечение защиты информации установленной технологией выполнения работ, исключающей утрату носителей информации и несанкционированный доступ к информации или к ее носителям, либо путем введения прямых правил, регулирующих организацию защиты информации от НСД.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 4 часа для очно-заочной формы обучения. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 4 курсе в 7 семестре для очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия (лабораторные работы), самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 5 семестре для очной формы обучения и контрольной работы и зачета с оценкой в 7 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05 Дисциплины по выбору Блок1.В.ДВ.5
Б1.В.ДВ.05.01 «Разработка политики

информационной безопасности в организациях»

Дисциплина «Разработка политики информационной безопасности в организациях» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и

контрольной работы и зачета в 8 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05.02 «Разработка политики информационной безопасности в Интернет - системах»

Дисциплина «Разработка политики информационной безопасности в Интернет-системах» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05.03 «Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ООО "НОВО")»

Дисциплина «Оценка защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа (ОАО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной безопасностью (СУИБ) для различных предприятий и организаций по защите информации по техническим каналам от НСД.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа, распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.05.04 «Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")»

Дисциплина «Контроль защищенности информации от утечки по техническим каналам (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Предмет изучения курса - практические правила по разработке политики безопасности и внедрению системы управления информационной безопасностью (СУИБ) для различных предприятий и организаций по защите информации по техническим каналам от НСД.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа , распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно - заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы

обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06 Дисциплины по выбору Блок1.В.ДВ.6

Б1.В.ДВ.06.01 «Организации защиты персональных данных на предприятии»

Дисциплина «Организация защиты персональных данных на предприятии» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины 4 зачетных единицы, 144 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.02 «Правовая охрана результатов интеллектуальной деятельности»

Дисциплина «Правовая охрана результатов интеллектуальной деятельности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины 4 зачетных единицы, 144 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.03 «Методы и средства защиты информации от утечки по техническим каналам (ООО "НОВО")»

Дисциплина «Методы и средства защиты информации от утечки по техническим каналам (ОАО «НОВО», НТЦ «ЗАРЯ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Цель изучение дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области защиты информации от утечки по техническим каналам.

В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на техническую защиту информационных объектов; 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 технической защиты информации; приобретение студентами навыков по практическому формированию мероприятий защиты информации от утечки по техническим каналам.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.06.04 «Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")»

Дисциплина «Средства защиты информации и оценка эффективности защиты от утечки по техническим каналам (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Цель изучение дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области защиты информации от утечки по техническим каналам.

В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на техническую защиту информационных объектов; 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 технической защиты информации; приобретение студентами навыков по практическому формированию мероприятий защиты информации от утечки по техническим каналам.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часов. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 7 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 7 семестре для очной формы обучения и контрольной работы и экзамена в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07 Дисциплины по выбору Блок1.В.ДВ.7

Б1.В.ДВ.07.01 «Защита профессиональной тайны в различных сферах деятельности»

Дисциплина «Защита профессиональной тайны в различных сферах деятельности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.02 «Информационная

безопасность операционных систем и баз данных»

Дисциплина «Информационная безопасность операционных систем и баз данных» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и

очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и контрольной работы и зачета в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.03 «Технические каналы утечки конфиденциальной информации (ООО "НОВО")»

Дисциплина «Технические каналы утечки конфиденциальной информации (ООО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Целью дисциплины является формирование знаний в области подготовки обучающихся по вопросам защиты информации от утечки по техническим каналам на объектах и в выделенных помещениях.

Содержание курса охватывает следующие темы:

Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Понятие и особенности утечки информации. Структура, классификация и основные

характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Распространение сигналов в технических каналах утечки информации Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС. Информационный конфликт (виды, варианты реализации). Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и зачета в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы

обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.07.04 «Технические каналы утечки информации (ООО "ЦБИ")»

Дисциплина «Технические каналы утечки конфиденциальной информации (ООО «ЦБИ»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Целью дисциплины является формирование знаний в области подготовки обучающихся по вопросам защиты информации от утечки по техническим каналам на объектах и в выделенных помещениях.

Содержание курса охватывает следующие темы:

Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Распространение сигналов в технических каналах утечки информации Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования. Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС. Информационный конфликт (виды, варианты реализации). Стратегии противоборствующих сторон в динамике развития информационного конфликта ТКС с системами воздействия. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и на 4 курсе в 8 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 6 семестре для очной формы обучения и зачета в 8 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.08 Дисциплины по выбору Блок1.В.ДВ.8

Б1.В.ДВ.08.01 «Лицензирование и сертификация в области защиты информации»

Дисциплина «Лицензирование и сертификация в области защиты информации» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

В курсе освещены вопросы организации и проведения работ с конфиденциальной информацией по лицензированию и сертификации деятельности предприятий, связанных с использованием сведений, составляющих государственную тайну, для данного предприятия, установленном нормативными правовыми актами и методологическими документами, получить лицензию на осуществление этого вида деятельности. Знание всех видов деятельности, подлежащих лицензированию в сфере защиты государственной тайны, алгоритм работы лицензирующего органа по лицензированию деятельности предприятий.

Целью курса является формирование навыков организации проведения комплекса мероприятий (лицензирования и сертификации), в результате которых устанавливается соблюдение требований законодательных и иных нормативных актов по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ; наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по ЗИ; наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

В курсе рассматриваются функции органов лицензирования и сертификации, испытательных центров, заявителей и их взаимодействие при проведении лицензирования объектов информатизации. Изучается порядок проведения лицензирования (разработка заявки на проведение лицензирования, программы и методики сертификационных испытаний, их проведение), оформление и регистрация лицензии соответствия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины

ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

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

Б1.В.ДВ.08.02 «Аттестация в области защиты информации»

Дисциплина «Аттестация в области защиты информации» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

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.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

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

Б1.В.ДВ.08.03 «Разработка объекта информатизации в защищенном исполнении (ООО "НОВО")»

Дисциплина «Разработка объекта информатизации в защищенном исполнении (ОАО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способность принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Содержание дисциплины охватывает круг вопросов, связанных с организацией работ на объекте информатизации в защищенном исполнении (ООО «НОВО»)», 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 данными). Анализируются изменения российского законодательства, последствия внесения изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой информационного ресурса и затрат на их защиту.

Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению функционирования объекта в защищенном исполнении с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности информационного объекта и используемых информационных технологий, способы снижения рисков утечки данных.

Общая трудоемкость освоения дисциплины 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.08.04 «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")»

Дисциплина «Разработка и сертификация средств защиты информации и технических средств в защищенном исполнении (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы

подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защита информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Содержание дисциплины охватывает круг вопросов, связанных с организацией работ на объекте информатизации в защищенном исполнении (ООО «НОВО»)», 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 данными). Анализируются изменения российского законодательства, последствия внесения изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой информационного ресурса и затрат на их защиту.

Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению функционирования объекта в защищенном исполнении с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности информационного объекта и используемых информационных технологий, способы снижения рисков утечки данных.

Общая трудоемкость освоения дисциплины 2 зачетных единицы, 72 часа. Практическая подготовка составляет 12/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 4 курсе в 8 семестре для очной формы обучения и в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 8 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно - заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Экономика информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09 Дисциплины по выбору Блок1.В.ДВ.9

Б1.В.ДВ.09.01 «Радиоэлектронные системы и средства как объекты информационной безопасности»

Дисциплина «Радиоэлектронные системы и средства как объекты информационной безопасности» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык», «Нормативные акты и стандарты по информационной безопасности», и компетенциях: ОПК-2,3,4,8,11; УК-4; ДОПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Цель изучение дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области радиоэлектронных основ информационной безопасности. В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на радиоэлектронную защиту информационных объектов; 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 радиоэлектронных основ информационной безопасности; приобретение студентами первичных навыков по практическому формированию мероприятий радиоэлектронной защиты объектов.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.02 «Основы радиоэлектронной разведки (РЭР)»

Дисциплина «Основы радиоэлектронной разведки (РЭР)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык» и компетенциях: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Цель изучение дисциплины является: - получение новых знаний и умений, повышения уровня профессиональной компетентности студентов в области радиоэлектронных основ информационной безопасности. В процессе изучения данного модуля необходимо учесть весь спектр научных воззрений на радиоэлектронную защиту информационных объектов; 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 радиоэлектронных основ информационной безопасности; приобретение студентами первичных навыков по практическому формированию мероприятий радиоэлектронной защиты объектов.

Содержание курса охватывает: демаскирующие признаки радиоэлектронных объектов и особенности их вскрытия технической разведкой; анализ радиоэлектронной обстановки на информационных объектах и основы технического контроля функционирования радиоэлектронных систем и средств; основные демаскирующие признаки радиоэлектронных объектов и особенности их вскрытия радиоэлектронной разведкой; анализ радиоэлектронной обстановки на информационных объектах и основы технического контроля функционирования радиоэлектронных систем и средств.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.03 «Методы и средства защиты информации от несанкционированного доступа (ООО "НОВО")»

Дисциплина «Методы и средства защиты информации от несанкционированного доступа (ООО «НОВО»)» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика»,

«Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Предмет изучения курса - методы и средства защиты информации от несанкционированного доступа.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа , распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа. Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.09.04 «Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")»

Дисциплина «Методы и средства обеспечения защищенности информации от несанкционированного доступа (ООО "ЦБИ")» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-2,3,4,11; УК-4.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Предмет изучения курса - методы и средства защиты информации от несанкционированного доступа.

Целью курса является формирование умения планировать и обосновывать мероприятия по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа , распределять роли и ответственности за обеспечение информационной безопасности, планировать измерение эффективности системы ЗИ.

Содержание курса последовательно раскрывает все этапы работы по разработке структуры и внедрению изменений в политику безопасности предприятия (организации), по оценке защищенности конфиденциальной информации по техническим каналам и от несанкционированного доступа. Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной формы обучения и на 5 курсе в 9 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета 5 семестре для очной формы обучения и контрольной работы и зачета в 9 семестре для очно-заочной формы обучения.

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

«Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10 Дисциплины по выбору Блок1.В.ДВ.10

Б1.В.ДВ.10.01 «Социотехносферная безопасность объектов информационной защиты»

Дисциплина «Социотехносферная безопасность объектов информационной защиты» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Целями изучения дисциплины являются: Дать студентам базовые знания по основам обеспечения социотехносферной безопасности ключевых объектов информационной защиты на предприятиях, организациях и учреждений 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 учреждений) с различными формами собственности с учетом современных подходов обеспечения информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 семестре для

очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена 6 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10.02 «Эффективность защищенных информационных систем»

Дисциплина «Эффективность защищенных информационных систем» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Дисциплина направлена на формирование следующих компетенций:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена 6 семестре для очной формы обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.10.03 «Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ООО "НОВО", ООО "ЦБИ")

Дисциплина «Методы и средства выявления демаскирующих признаков закладочных устройств в защищаемых помещениях (ОАО «НОВО». НТЦ «ЗАРЯ») относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется базовой кафедрой защиты информации.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная

безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Разработка политики информационной безопасности в организациях», «Организация защиты персональных данных на предприятии» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9; ПК-1,2,3,4.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-4. Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

В курсе освещены вопросы организации и проведения работ с конфиденциальной информацией по выявлению демаскирующих признаков закладочных устройств в защищаемых помещениях лицензированию и сертификации деятельности предприятий, связанных с использованием сведений, составляющих конфиденциальную информацию, для данного предприятия, установленном нормативными правовыми актами и методологическими документами.

Целью курса является формирование навыков организации проведения комплекса мероприятий направленных на выявление демаскирующих признаков закладочных устройств в защищаемых помещениях, в результате которых устанавливается соблюдение требований законодательных и иных нормативных актов по обеспечению защиты сведений, составляющих конфиденциальную информацию, в процессе выполнения работ; наличие в структуре предприятия подразделения по защите конфиденциальной информации и необходимого числа специально подготовленных сотрудников для работы по ЗИ; наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часа. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 3 курсе в 6 семестре для очной формы обучения и в 10 семестре для очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и экзамена в 6 семестре для очной формы

обучения и контрольной работы и экзамена в 10 семестре для очно-заочной формы обучения.

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

Б1.В.ДВ.11 Дисциплины по выбору Блок1.В.ДВ.11

Б1.В.ДВ.11.01«Введение в профессию»

Дисциплина «Введение в профессию» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета с оценкой в 1 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Безопасность информационных технологий», «Гуманитарные аспекты (профессиональная этика) информационной безопасности», «Базы данных, системы управления

базами данных», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Б1.В.ДВ.11.02 «Профессиональные адаптации инвалидов и лиц с ОВЗ»

Дисциплина «Профессиональная адаптация инвалидов и лиц с ОВЗВ» относится к обязательным дисциплинам части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на общих знаниях и коммуникативных компетенциях, полученных в средних образовательных учреждениях.

Дисциплина направлена на формирование следующих компетенций:

УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

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.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Практическая подготовка составляет 16/12 ч. для очной и очно-заочной форм обучения соответственно. Преподавание дисциплины ведется на 1 курсе в 1 семестре для очной и очно-заочной формы обучения и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме контрольной работы и зачета в 1 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Безопасность информационных технологий», «Гуманитарные аспекты (профессиональная этика) информационной безопасности», «Базы данных, системы управления

базами данных», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Блок 2. Практика

В соответствии ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» раздел ОПОП ВО «Практики» является обязательным. Основной целью проведения практики является закрепление и углубление знаний, полученных студентами в ходе теоретического обучения, развитие и накопление специальных практических навыков для решения профессиональных задач. Она представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Практическая подготовка – форма организации образовательной деятельности при освоении ОПОП в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю ОПОП.

Полнота и степень детализации практик регламентируется программами практик применительно к особенностям конкретных баз практик. При реализации данной программы по направлению подготовки 10.03.01«Информационная безопасность» предусматриваются следующие виды практик:

учебная практика: ознакомительная практика; учебно-лабораторная практика.

производственная практика: технологическая практика; преддипломная практика.

Учебные и производственные практики проводятся на базе: ООО «Клио», НИИ КС им. А. А. Максимова - филиала ФГУП «ГКНПЦ им М. В. Хруничева», кафедры «Информационной безопасности, отдела защиты информации и секретного делопроизводства Министерства финансов Московской области, г. Москва, ЦБИ г. Юбилейный, ТРВ, РКК «Энергия», ОАО «НОВО», НТЦ «ЗАРЯ».

Практики планируются в соответствии с графиком учебного процесса и программами практик. От общей трудоемкости ОПОП ВО подготовки бакалавра (240 зачетных единиц) на практику предусматривается 648 часов 18 зачетных единиц (учебная практика 216 часов 6 зачетных единиц, а производственная практика 432 часа 12 зачетных единиц).

В процессе проведения всех видов практики основное внимание уделяется формированию у студентов универсальных и профессиональных компетенций, позволяющих самостоятельно повышать уровень профессиональных знаний.

По итогам каждой из практик проводится аттестация: каждый студент представляет письменный отчет, дневник практики, характеристику

руководителя практики о качестве ее прохождения; проводится обсуждение хода практики и ее результатов на кафедре, а также самооценка студента. На основании обсуждения результатов выставляется дифференцированная оценка.

Программы учебной и производственной практик приведены в Приложении 5, 6, 7.

Обязательная часть
Б2.В.01(П) Преддипломная практика

Производственная (преддипломная) практика (6 недель, (324 часа), 9 зачетных единиц) проводится на 4 курсе в восьмом семестре для очной формы обучения и на 5 курсе в девятом семестре для очно-заочной формы обучения с целью углубления и закрепления профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;
ДОПК-1. Способен проводить анализ функционального процесса объекта информатизации с целью выявления возможных угроз, их вероятных целей, путей реализации и предполагаемого ущерба;
ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ДОПК-3. Способен разработать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ДОПК-4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

Производственная (преддипломная) практика проводится с целью ознакомления студентов с существующей системой информационной безопасности реального информационного объекта, с методами, средствами и силами, используемыми в этой системе, закрепления, расширения, углубления и систематизации знаний по общепрофессиональным дисциплинам, изученным студентами в соответствии с учебным планом в течение 1, 2, 3 и 4 курсов, в число которых входят такие дисциплины, как «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» и др., подготовка у студентов практической базы для осознанного изучения специальных дисциплин, отражающих специфику их будущей работы, которые будут изучаться ими в рамках учебного плана четвертого курса. В их число входят такие дисциплины, как «Информационная безопасность предприятия», «Инженерно-техническая защита информации», «Технические средства охраны» и другие, осуществить сбор материалов, которые можно будет использовать в дальнейшем при курсовом проектировании и написании выпускной квалифицированной работы.

Производственная (преддипломная) практика проводится на базе ЗАО «Клио», «НИИ КС им. А. А. Максимова» - филиала ФГУП «ГКНПЦ им М. В. Хруничева», 18 ЦНИИ МО, кафедры «Информационной безопасности», лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности, ООО «НОВО», НТЦ «ЗАРЯ», ООО «ЦБИ».

Итогом проведения производственной (преддипломной) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях информационной безопасности (защиты информации) в специальных подразделениях по защите информации, заполнения специальной документации и подготовка материалов для написания ВКР.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в восьмом для очной формы обучения и зачета с оценкой в девятом семестре для очно-заочной формы обучения.

Часть, формируемая участниками образовательных отношений

Б2.В.01 (У) Ознакомительная практика

Учебная (по получению первичных профессиональных умений и навыков) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 1 курсе во втором семестре для очной и на 2 курсе в четвертом семестре для очно-заочной формы обучения с целью углубления и закрепления первичных

профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;
УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;
ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;

Практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищённые информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 1 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности

Учебная практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.

Итогом проведения учебной практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях подразделений информационной безопасности (защиты информации), заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой во втором семестре для очной и в четвертом семестре для очно-заочной формы обучения.

Б2.В.02(У) Учебно-лабораторная практика

Учебная (технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 2 курсе в четвертом семестре для очной и на 3 курсе в шестом семестре для очно-заочной формы обучения с целью углубления и закрепления первичных профессиональных знаний и навыков, полученных при теоретическом обучении и формирования компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищённые информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 2 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности

Учебная (технологическая) практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности.
Итогом проведения учебной (технологической) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях подразделений информационной безопасности (защиты информации), заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в четвертом семестре для очной и в шестом семестре для очно-заочной формы обучения.

Б2.В.03 (П) Технологическая практика

Производственная (проектно-технологическая) практика (2 недели, (108 часов), 3 зачетных единицы) проводится на 3 курсе в шестом семестре для очной и на 4 курсе в восьмом семестре для очно-заочной формы обучения, с целью углубления и закреп навыков, полученных при теоретическом обучении и формирования компетенций:

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-3. Разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;
ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Производственная практика проводится с целью отработки студентами навыков решения задач по защите информации на современном компьютерном оборудовании и в сетях, закрепление теоретических знаний, полученные по дисциплинам: «Теоретические основы защиты информации», «Защищённые информационные технологии», ознакомление студентов с основными методами защиты информации на персональных компьютерах и в сетях в качестве индивидуального пользователя, расширения и систематизации знаний по специализированным дисциплинам, изученным студентами в соответствии с учебным планом в течение 3 курса и подготовка студентов к дальнейшему углубленному изучению дисциплин своей специализации, а также расширение их круга знаний в области защиты информации и применения различных методов, процедур и пакетов программ для решения различных задач информационной безопасности.

Производственная (проектно-технологическая) практика проводится на базе лабораторий кафедры «Информационной безопасности»: Аудитория 2210: Лаборатория управления информационной безопасности; Аудитория 2210а: Лаборатория защищенных технических средств и систем; Аудитория 2206: Лаборатория технологий обеспечения информационной безопасности, на базе ЗАО «Клио», «НИИ КС им. А. А. Максимова» - филиала ФГУП

«ГКНПЦ им М. В. Хруничева», 18 ЦНИИ МО, ООО «НОВО», НТЦ «ЗАРЯ», ООО «ЦБИ».

Итогом проведения производственной (проектно-технологической) практики является овладение студентами навыками использования контрольно-проверочной аппаратуры, программных продуктов, применяемых в целях информационной безопасности (защиты информации) в специальных подразделениях по защите информации, заполнения специальной документации.

Программой предусмотрены следующие виды контроля: промежуточная аттестация в форме зачета с оценкой в шестом семестре для очной и в восьмом семестре для очно-заочной формы обучения.

ФТД. Факультативы

Факультативные дисциплины призваны углублять, расширять научные и прикладные знания обучающихся в соответствии с их потребностями, приобщать их к исследовательской деятельности, создавать условия для самоопределения личности и ее самореализации, обеспечивать разностороннюю подготовку профессиональных кадров.

Выбор факультативных дисциплин проводится обучающимися самостоятельно, в соответствии с их потребностям.

ФТД.В.01 «Технико-экономическое обоснование проекта»

Дисциплина «Технико-экономическое обоснование проекта» относится к факультативным дисциплина основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Криптографические методы защиты информации», а также компетенциях и компетенциях: УК-5; ОПК-1,5,6,8,9,13; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;

ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Целью курса является формирование знаний основам проектной деятельности. Выявлению существующих проблем в рамках обеспечения функционирования объекта информатизации и подготовке предложений по приведению существующей системы информационной безопасности объекта в соответствие требованиям предъявляемых регуляторами к таким системам в соответствии с существующей нормативной базой и представленными на рынке средствами обеспечения информационной безопасности объектов информатизации.

Содержание курса связано с разработкой обоснованных предложений по совершенствованию механизмов защиты обрабатываемого ресурса на предприятии (организации).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 3 курсе в 5 семестре для очной и очно-заочной форм обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета в 5 семестре для очной и очно-заочной формы обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Разработка и реализация проекта», «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

ФТД.В.02 «Разработка и реализация проекта»

Дисциплина «Разработка и реализация проекта» относится к факультативным дисциплина основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «История», «Основы права», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Конфиденциальное делопроизводство и защищенный электронный документооборот», «Криптографические методы защиты информации», а также компетенциях и компетенциях: УК-5; ОПК-1,5,6,8,9,13; ДОПК-1,3.

Дисциплина направлена на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;
ПК-5. Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Целью курса является формирование знаний основам проектной деятельности. Обоснование предложений по приведению системы информационной безопасности объекта информатизации в соответствие с уточненными требованиями предъявляемые к такого рода системам в соответствии с существующей нормативно-правовой базой.

Содержание курса связано с разработкой обоснованных предложений по совершенствованию механизмов защиты обрабатываемого ресурса на предприятии (организации). Проведение технико-экономических обоснований предлагаемых вариантов решения выявленных проблем, связанных с обеспечением системы информационной безопасности объекта информатизации. Осуществление нормативно-правого закрепления предложений в существующей системе документационного обеспечения управления предприятием (организацией) в рамках бесперебойного, функционирования системы информационной безопасности объекта информатизации.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа. Преподавание дисциплины ведется на 3 курсе в 6 семестре и 4 курсе в 7 семестре для очной и очно-заочной форм обучения и предусматривает проведение учебных занятий следующих видов: практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрены следующие виды контроля: два текущих контроля успеваемости в форме тестирования и промежуточная аттестация в форме зачета и курсового проекта в 6 семестре и зачета с оценкой и курсового проекта в 7 семестре для очной и очно-заочной форм обучения.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Разработка и

реализация проекта», «Информационно-психологическая безопасность персонала предприятия», «Защита общества от информации, запрещенной к распространению», «Разработка политики информационной безопасности в организациях», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.