

#### 4.9. Аннотации дисциплин

##### **Б1. Дисциплины (модули)**

###### **Базовая часть**

Дисциплина «**Экономика и управление**» **Б1.Б.01** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах: «История», «Философия», «Информатика», «Экономика».

Дисциплина реализуется кафедрой экономики

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-12: способность организовать работу коллектива исполнителей, принимать управленческие решения;

Содержание дисциплины охватывает круг вопросов, связанных с изучением сущности и факторов риска, классификацией рисков, системой управления рисками, идентификацией и анализом рисков, методами управления риском, оценкой эффективности методов управления риском.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения в дальнейшем дисциплин «Экономико-управленческие аспекты обеспечения информационной безопасности», отдельных разделов дисциплины «Теоретические основы управления», для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы магистра.

Дисциплина «**Специальные разделы математики**» **Б1.Б.02** относится к базовой части блока 1 адаптированной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой Математики и естественнонаучных дисциплин.

Дисциплина базируется на курсах «Математика (математический анализ, алгебра, геометрия)», «Теория вероятностей и математическая статистика» изученных в бакалавриате.

Знания и умения, полученные студентами при изучении дисциплины, необходимы при изучении таких дисциплин, как «Математическое моделирование технических объектов и систем управления», «Экономико – управленческие аспекты обеспечения информационной безопасности», «Методы оценки криптографических систем защиты информации», «Компьютерное моделирование информационных процессов и технологий».

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность к абстрактному мышлению, анализу, синтезу;

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-1: способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с изучением теории экстремальных задач, нелинейного программирования, вариационного исчисления, оптимального управления.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета с оценкой.

Дисциплина **«Специальные разделы физики» Б1.Б.03** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина базируется на курсах «Физика», «Математика (математический анализ, алгебра, геометрия)», изученных в бакалавриате.

Дисциплина реализуется кафедрой математики и естественнонаучных дисциплин.

Знания и умения, полученные студентами при изучении дисциплины, необходимы при изучении таких дисциплин, как «Инструментальные методы выявления технических каналов утечки информации».

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

Содержание дисциплины охватывает круг вопросов, связанных с изучением физических полей объектов, акустики, антенн, основ радиолокации.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета.

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

Дисциплина **«Защищенные информационные системы» Б1.Б.04** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах: «Основы информационной безопасности», «Основы исследований информационной безопасности».

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в

соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

Содержание дисциплины охватывает круг вопросов, связанных с изучением проблем информационной безопасности в условиях становления современного информационного общества, использованием организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующих создание и использование средств защиты информации, получением навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе в 1 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен контроль успеваемости в виде контрольной работы и экзамена.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин: “Управление информационной безопасностью“, “Информационно-аналитические системы безопасности“, “Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем“ и выполнении выпускной квалификационной работы магистра.

Дисциплина **«Технологии обеспечения информационной безопасности объектов» Б1.Б.05** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах: “Основы информационной безопасности”, “Основы исследований информационной безопасности“, “ Информационная безопасность автоматизированных систем” и компетенциях ОК-5; ОПК-2,3,4; ПК-2,5,8,9,11,12,15.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и

средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

Содержание дисциплины охватывает круг вопросов, связанных с изучением концептуальных и методологических основ в области теории обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрен контроль успеваемости в форме контрольной работы и экзамена.

Основные положения дисциплины должны быть использованы для написания магистерской диссертации.

Дисциплина **«Управление информационной безопасностью» Б1.Б.06** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности в 3-м семестре.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах: “Основы информационной безопасности”, “Основы исследований информационной безопасности“, “ Информационная безопасность автоматизированных систем” и на дисциплинах, изученных ранее в магистратуре: “Экономика и управление”, “Защищенные информационные системы”, «Теория игр и исследование операций», «Теоретические основы компьютерной безопасности» и компетенции ОК-2; ОПК-2, ПК-1,2,5,7,8,12,14,15

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности;

ПК-8: способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-11: способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины включает в себя политику информационной безопасности региона и отдельных региональных структур (объектов, процессов); базовые основы процессов и систем управления информационной безопасностью; организационно-кадровые и технические аспекты управления информационной безопасностью; основы оценки эффективности управления информационной безопасностью.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрен контроль успеваемости в форме контрольной работы и зачета с оценкой.

Основные положения дисциплины должны быть использованы для написания магистерской диссертации.

Дисциплина «**Методы и средства защиты информации в системах электронного документооборота**» **Б1.Б.07** относится к вариативной части, устанавливаемой вузом, блока адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: “Экономика и управление”, “Защищенные информационные системы”, “Основы теории информационной безопасности“, «Методы и средства обеспечения безопасного доступа к информационным ресурсам» и компетенциях ОК-2, ОПК-2, ПК-1,5,7,8,12,13,14,15.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

Содержание дисциплины охватывает понятие и особенности конфиденциальной информации. Общую характеристику нормативной правовой базы. Документирование конфиденциальной информации конфиденциальных дел. Организацию конфиденциального документооборота. Разрешительную систему доступа к конфиденциальной информации. Составление номенклатуры дел, формирование и оформление Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе, в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрен текущий контроль успеваемости в виде экзамена.

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

Дисциплина **«Деловой иностранный язык» Б1.Б.08** относится к базовой части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой иностранных языков.

Дисциплина базируется на ранее изученных дисциплинах бакалавриата: «Русский язык и культура речи», «Иностранный язык», и компетенциях ОК-2,7; ОПК-4. .

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность к абстрактному мышлению, анализу, синтезу;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

Данный курс, рассчитанный на один учебный семестр, и является первым этапом формирования языковой компетенции в сфере деловой коммуникации на иностранном языке.

Содержание охватывает деловые коммуникации и управление кросс-культурными различиями. Практическое применение информационных технологий.

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

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета с оценкой.

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

#### Б1.В. Вариативная часть

Дисциплина **«Современная философия и методология науки»**

**Б1.В.01** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Дисциплина реализуется кафедрой Гуманитарных и социальных дисциплин.

Освоение курса базируется на дисциплинах программы подготовки бакалавров, изученных студентом ранее: «Философия», «История», «Правоведение».

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность к абстрактному мышлению, анализу, синтезу;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;



ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

Содержание дисциплины охватывает круг вопросов, связанных с пониманием роли современной философии в развитии науки и профессиональной деятельности, применением методологии науки для анализа проблем управления качеством, совершенствованием и развитием интеллектуального и общекультурного уровня магистров.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 1 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета.

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

Дисциплина **«Математическое моделирование технических объектов и систем управления» Б1.В.02** относится к вариативной части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой Математики и естественнонаучных дисциплин.

Дисциплина базируется на курсах, изученных ранее в бакалавриате: «Математика (математический анализ, алгебра, геометрия)», «Теория вероятностей и математическая статистика».

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

Содержание дисциплины охватывает круг вопросов, связанных с изучением имитационного моделирования, моделирования операций по схеме марковских случайных чисел, систем массового обслуживания и их применения в моделировании.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета.

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

Дисциплина **«Теория игр и исследование операции» Б1.В.03** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность» кафедрой Математики и естественно-научных дисциплин.

Дисциплина базируется на курсах, изученных ранее в бакалавриате «Математика (математический анализ, алгебра, геометрия)», «Теория вероятностей и математическая статистика».

Дисциплина направлена на формирование следующих компетенций:

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

Содержание дисциплины охватывает круг вопросов, связанных с изучением построения математических моделей многих реальных явлений и процессов, изучаемых в различных прикладных технических и экономических науках.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе во 2 семестре и предусматривает проведение учебных занятий следующих видов:

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

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин “Методы оценки криптографических систем защиты информации”, “Экономико-управленческие аспекты обеспечения информационной безопасности”, для прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы магистра.

Дисциплина «**Теоретические основы управления**» **Б1.В.04** относится к дисциплинам вариативной части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на одновременно изучаемых дисциплинах: «Специальные разделы математики»; «Специальные разделы физики»; «Современная философия и методология науки»; «Защищенные информационные системы» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,3,4,5,6,7,8,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: концептуально-теоретические основы информационной безопасности; методологические и практические основы управления системами, процессами и объектами; моделирование, математическое описание и анализ систем, процессов и элементов управления с помощью систем дифференциальных уравнений, переходных функций и интегральных преобразований; управление проектами и проектными рисками; организация и управление материальными потоками,

запасами и их распределением; особенности управления и регулирования информационной сферой; перспективы развития теории и практики управления.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, во в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы и зачета.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин, как “Организационно-правовые механизмы обеспечения информационной безопасности”, “Информационно-аналитические системы безопасности” и для написания магистерской диссертации.

**Дисциплина «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» Б1.В.05** относится к вариативной части, устанавливаемой вузом, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности. Дисциплина базируется на одновременно изучаемых дисциплинах: «Специальные разделы математики»; «Специальные разделы физики»; «Современная философия и методология науки»; «Защищенные информационные системы» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,3,4,5,6,7,8,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-1: способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности;

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; Содержание дисциплины охватывает два раздела: раздел (модуль) 1. Интеллектуальные информационные системы (ИИС). Назначение, классификация ЭСКОБ и использование для комплексной оценки безопасности автоматизированных телекоммуникационных систем. раздел 2. Проектирование, тестирование и развитие ЭСКОБ автоматизированных телекоммуникационных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 1 курсе, во в 2 семестре, и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрен текущий контроль успеваемости в форме контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин «Технология обеспечения информационной безопасности», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» и выполнении выпускной квалификационной работы магистра.

Дисциплина **«Организационно-правовые механизмы обеспечения информационной безопасности» Б1.В.06** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы теории информационной безопасности», «Защищённые информационные системы» и компетенциях: ОК-2 и ПК-1,5,14.

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: Введение. Содержание основных научных понятий и категорий теории безопасности. Угрозы информации. Информация как объект защиты (организационно – правовой аспект). Концептуальные документы в области защиты информации. Основные федеральные нормативные правовые акты. Основные подзаконные акты в области защиты информации. Система государственных и отраслевых требований (стандартов) в области защиты информации. Особенности зарубежных стандартов защиты информации (организационно – правовой аспект). Нормативные документы ФСТЭК России (организационно – правовой аспект). Общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Проведение сертификационных испытаний (организационно – правовой аспект). Аттестация объектов информатизации. Сертификация продукции, ввозимой из-за границы. Сертификация на региональном и международном уровнях (организационно – правовой аспект). Служба информационной безопасности предприятия (организационно – правовой аспект).

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины необходимы при выполнении выпускной квалификационной работы магистра.

Дисциплина **«Теоретические основы компьютерной безопасности» Б1.В.07** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: ОК-2 и ПК-1,5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

Содержание дисциплины охватывает: Раздел 1. Концептуально-теоретические основы компьютерной безопасности. Раздел 2. Прикладные основы теории компьютерной безопасности.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе, во 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, лабораторные работы, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Информационная безопасность финансово-кредитных структур», «Комплексная проверка информационной безопасности» и для написания магистерской диссертации.

Дисциплина **«Информационно-аналитические системы безопасности» Б1.В.08** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на одновременно изучаемых дисциплинах: «Методы и средства обеспечения безопасного доступа к информационным ресурсам», «Защищенные информационные системы» и компетенциях: ОК-2 и ПК-5,7,8,13,14,16.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты,

прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-13: способность организовать управление информационной безопасностью;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: Раздел 1. Основы проектирования и внедрения ИАС безопасности региона. Раздел 2. Информация: сбор, защита, анализ для региональной ИАС безопасности

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе 3 семестр и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы при выполнении выпускной диссертационной работы магистра.

Дисциплина «**Теория систем и системный анализ**» **Б1.В.09** относится к вариативной части, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Дисциплина базируется на ранее изученных дисциплинах: «Теоретические основы управления», «Современная философия и методология науки» и компетенциях: ОК-1, ОПК-2 и ПК-5,6,7,8,13,14,15,16.

Дисциплина направлена на формирование следующих компетенций:

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в



соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: Понятия о системном подходе, системном анализе. Выделение системы из среды, определение системы. Оптимизация систем и системное проектирование. Системы и закономерности их функционирования и развития. Системный подход как методология управления сложными системами. Управляемость, достижимость, устойчивость. Классификация систем. Естественные, концептуальные и искусственные, простые и сложные, целенаправленные, целеполагающие, активные и пассивные, стабильные и развивающиеся системы. Поведение, деятельность и организация систем. Особенности применения обобщенного алгоритма. Формирование и анализ моделей. Выявление топологии системы. Свойства системы. Целостность и структуризация, связность, структура, организация, интегрированные качества. Системное моделирование. Основные проблемы теории систем. Модели и моделирование. Управление системой. Модели систем. Обоснование класса допустимых систем. Статические, динамические, концептуальные, формализованные (процедуры формализации моделей систем), информационные, логико-лингвистические, семантические и др. Роль человека в решении задач системного анализа.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины, необходимы при выполнении выпускной диссертационной работы магистра.

Дисциплина **«Профессиональный иностранный язык» Б1.В.10** относится к вариативной части блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01. «Информационная безопасность».

Дисциплина реализуется кафедрой иностранных языков.

Изучение иностранного языка строится на междисциплинарной основе, предполагая интеграцию знаний из различных предметных дисциплин, одновременное развитие как собственно коммуникативных, так и

профессионально-коммуникативных, информационных, академических и социальных умений.

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность к абстрактному мышлению, анализу, синтезу;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок.

Содержание дисциплины охватывает: деловые коммуникации и управление кросс - культурными различиями. Практическое применение информационных технологий.

Данный курс, рассчитанный на один учебный семестр, и является первым этапом формирования языковой компетенции в сфере профессиональной коммуникации на иностранном языке.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часа. Преподавание дисциплины ведется на 1 курсе в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде экзамена и контрольной работы.

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

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

Дисциплина **«Экономико-управленческие аспекты обеспечения информационной безопасности» Б1.В.ДВ.01.01** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Специальные разделы математики»; «Теоретические основы управления»; «Защищенные информационные системы»; «Экономика и управление» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,5,12,13,14,15,16.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

Содержание дисциплины охватывает круг вопросов, связанных с формированием у обучаемых концептуальных и методологических подходов в области экономико-управленческих основ обеспечения информационной безопасности региона в процессе развития современного информационного общества.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре, соответственно и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрен контроль успеваемости в форме экзамена.

Знания и компетенции, полученные при освоении дисциплины необходимы при выполнении выпускной диссертационной работы магистра.

Дисциплина **«Методы оценки криптографических систем защиты информации» Б1.В.ДВ.01.02** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Защищенные информационные системы», «Основы теории информационной безопасности», «Анализ статистической информации с помощью пакета прикладных программ» и компетенциях: ОК-2, ПК-1,3,4,5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с изучением современных методов и средств криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности, освоением студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрен контроль успеваемости в виде контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины необходимы при выполнении выпускной диссертационной работы магистра.

Дисциплина **«Концепция построения комплексных систем защиты информации хозяйствующих субъектов (ОАО «НОВО», НТЦ «ЗАРЯ»)» Б1.В.ДВ.01.03** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Защищенные информационные системы», «Основы теории информационной безопасности», «Анализ статистической информации с помощью пакета прикладных программ» и компетенциях: ОК-2, ПК-1,3,4,5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования в профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты,

прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с применением на практике современных методов и средств криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности, освоением студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрен контроль успеваемости в виде контрольной работы и экзамена.

Знания и компетенции, полученные при освоении дисциплины необходимы при выполнении выпускной диссертационной работы магистра.

## **Б1.В.ДВ. 02 Дисциплины по выбору Блок 1.В.ДВ.2**

Дисциплина «**Основы теории информационной безопасности**» **Б1.В.ДВ.02.01** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах «Основы исследований информационной безопасности»,

“Основы информационной безопасности”, на одновременно изучаемых дисциплинах: «Защищенные информационные системы» и компетенциях: ОК-2, ПК-5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества.

Содержание дисциплины охватывает: современные проблемы информационной безопасности. Научно-методологические основы интенсификации процессов информационной безопасности. Теоретико-методологические основы оценки угроз и уязвимостей информационных объектов. Методологические основы определения требований к информационной безопасности. Методология формирования комплексных систем информационной безопасности. Особенности управления информационной безопасностью. Перспективы развития теории и практики информационной безопасности

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часов. Преподавание дисциплины ведется на 1 курсе 1 семестр и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, экзамена, контрольной работы.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин «Информационная безопасность финансово-кредитных структур», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» и для написания магистерской диссертации.

Дисциплина **«Методы и средства обеспечения безопасного доступа к информационным ресурсам» Б1.В.ДВ.02.02** относится к вариативной части дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах “Основы исследований информационной безопасности”, “Основы информационной безопасности”, на одновременно изучаемых

дисциплинах: «Защищенные информационные системы» и компетенциях: ОК-2, ПК-5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: Методологию проектирования систем информационной безопасности региона. Особенности проектирования систем защиты информации регионального уровня. Основы моделирования систем информационной безопасности региона. Методику оценки эффективности проектируемых систем информационной безопасности. Особенности проектирования адаптивных систем информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часов. Преподавание дисциплины ведется на 1 курсе 1 семестр и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, экзамена и контрольной работы.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» и для написания магистерской диссертации.

**Дисциплина «Основы организации и обеспечения специальных работ по выявлению закладочных устройств (ОАО «НОВО», НТЦ «ЗАРЯ»)**

**Б1.В.ДВ.02.03** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах «Основы исследований информационной безопасности», «Основы информационной безопасности», на одновременно изучаемых дисциплинах: «Защищенные информационные системы» и компетенциях: ОК-2, ПК-5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-13: способность организовать управление информационной безопасностью;

ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: 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.



Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы, 144 часов. Преподавание дисциплины ведется на 1 курсе 1 семестр и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, экзамена и контрольной работы.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» и для написания магистерской диссертации.

### **Б1.В.ДВ. 03 Дисциплины по выбору Блок 1.В.ДВ.3**

Дисциплина «**Информационная безопасность финансово-кредитных структур**» **Б1.В.ДВ.03.01** относится к вариативной части дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: “Экономика и управление”, “Основы теории информационной безопасности“, “Защищённые информационные системы“ и компетенциях: ОК-2, ОПК-2 и ПК-1,5,12,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности.

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).

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 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе, в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольная работа, зачет.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

Дисциплина **«Комплексная проверка информационной безопасности» Б1.В.ДВ.03.02** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность»

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы теории информационной безопасности»; «Специальные разделы физики»; «Теоретические основы компьютерной безопасности»; «Защищенные информационные системы» и компетенциях: ОК-2, ОПК-2 и ПК-1,3,4,5,7,8,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

Содержание дисциплины охватывает: основные положения по комплексному аудиту информационной безопасности. Характеристика направлений и проблемы комплексного аудита региональной информационной безопасности. Нормативно-правовая база комплексного аудита информационной безопасности органов управления регионом. Методика комплексного аудита информационной безопасности объектов управления регионом. Лицензирование деятельности объектов и сертификация систем защиты в области региональной информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе, в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольная работа, зачет.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

Дисциплина **«Основы управления корпоративной информационной безопасностью» (ОАО «НОВО», НТЦ «ЗАРЯ») Б1.В.ДВ.03.03** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность»

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы теории информационной безопасности»; «Специальные разделы физики»; «Теоретические основы компьютерной безопасности»; «Защищенные информационные системы» и компетенциях: ОК-2, ОПК-2 и ПК-1,3,4,5,7,8,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

Содержание дисциплины охватывает: 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 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе, в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольная работа, зачет.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

#### **Б1.В.ДВ. 04 Дисциплины по выбору Блок 1.В.ДВ.4**

Дисциплина «**Анализ статистической информации с помощью пакета прикладных программ**» **Б1.В.ДВ.04.01** относится к вариативной части, дисциплины по выбору блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой гуманитарных и социальных дисциплин.

Дисциплина базируется на ранее изученных дисциплинах: «Экономика и управление»; «Специальные разделы математики» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,12.

Дисциплина направлена на формирование следующих компетенций: ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности.

Содержание дисциплины охватывает проблемы практического усвоения студентами принципов компьютерной обработки массивов данных, методам статистического анализа, анализу одномерных и двумерных распределений, табличному и графическому представлению данных. Особое внимание уделяется изучению методических и компьютерных аспектов использования программного комплекса SPSS для обработки массивов данных и представления результатов анализа в виде таблиц и графиков.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы при освоении одновременно изучаемых дисциплин «Информационно-аналитические системы безопасности», «Экономико-управленческие аспекты обеспечения информационной безопасности» и для написания магистерской диссертации.

Дисциплина **Социальная инженерия в информационной безопасности» Б1.В.ДВ.04.02** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности. Дисциплина базируется на ранее изученных дисциплинах: «Современная философия и методология науки»; «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: ОК-1,2 и ПК-1,5,6,7,8,14.

Дисциплина направлена на формирование следующих компетенций:  
ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание дисциплины охватывает: введение. Социальная инженерия как технология несанкционированного доступа к информации или системам хранения информации без использования технических средств.

Техники и термины социальной инженерии, используемые для несанкционированного доступа к конфиденциальной информации.

Теоретико-методологические основы оценки уязвимости информационных объектов с учетом возможных воздействий с использованием технологии социальной инженерии. Методологические основы определения требований к информационной безопасности с учетом возможностей и развития технологии социальной инженерии. Методология формирования комплексных систем информационной безопасности против атак со стороны социального хакерства. Особенности управления информационной безопасностью в условиях воздействия со стороны социальной инженерии. Перспективы развития теории и практики информационной безопасности с учетом противодействия несанкционированному доступу к информации с использованием технологии социальной инженерии

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы при освоении одновременно изучаемых дисциплин “Организационно-правовые механизмы обеспечения информационной безопасности, “Экономико-управленческие аспекты обеспечения информационной безопасности” и для написания магистерской диссертации.

Дисциплина **«Государственная система защиты информации в части проведения специальных работ (ОАО «НОВО», НТЦ «ЗАРЯ»)»** **Б1.В.ДВ.04.03** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Современная философия и методология науки»; «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: ОК-1,2 и ПК-1,5,6,7,8,14.

Дисциплина направлена на формирование следующих компетенций:

ПК-1: способность понимать и анализировать направления развития информационных телекоммуникационных технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

ПК-12: способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения;

ПК-13: способность организовать управление информационной безопасностью;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

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, исключаяющей 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 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, в 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.



Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы при освоении одновременно изучаемых дисциплин “Организационно-правовые механизмы обеспечения информационной безопасности, “Экономико-управленческие аспекты обеспечения информационной безопасности” и для написания магистерской диссертации.

### **Б1.В.ДВ. 05 Дисциплины по выбору Блок 1.В.ДВ.5**

Дисциплина «**Инструментальные методы выявления технических каналов утечки информации**» **Б1.В.ДВ.05.01** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: “Специальные разделы физики”, “Технологии обеспечения информационной безопасности объектов”, “Методы и средства обеспечения безопасного доступа к информационным ресурсам” и компетенциях: ОПК-2, ПК-3,4,6,7,8,13,14,15,16.

Дисциплина направлена на формирование следующих компетенций:

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

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 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре

и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

Дисциплина **«Компьютерное моделирование информационных процессов и технологий» Б1.В.ДВ.05.02** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управления.

Дисциплина базируется на ранее изученных дисциплинах «Основы теории информационной безопасности», «Специальные разделы математики», «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,5,6,7,8,15.

Дисциплина направлена на формирование следующих компетенций:

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

Содержание охватывает определение и назначение моделирования. Цель и задачи компьютерного моделирования информационных процессов. Определение моделей, их свойства и классификация. Математическое моделирование и его место в теории познания. Критерии оценок качества моделирования. Этапы построения математической модели и решения задачи математического моделирования. Обследование объекта моделирования. Математическая постановка задачи моделирования и построение модели информационного процесса. Выбор и обоснование метода решения задачи. Реализация математической модели в виде программы. Проверка адекватности построенной модели. Проведение моделирования информационных процессов и анализ его результатов. Примеры

математических моделей и значимость результатов полученных с их помощью в результате математического моделирования. Моделирование в условиях неопределенностей. Причины неопределенностей и их виды. Моделирование в условиях стохастической неопределенности и неопределенностей описываемых с позиции теории чувствительности.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

Дисциплина **«Комплексный аудит информационной безопасности автоматизированных систем (ОАО «НОВО», НТЦ «ЗАРЯ»)» Б1.В.ДВ.5.3** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управления.

Дисциплина базируется на ранее изученных дисциплинах «Основы теории информационной безопасности», «Специальные разделы математики», «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,5,6,7,8,15.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;
- ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;
- ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;
- ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

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 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 2 курсе в 3 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета и контрольной работы.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

### **Б1.В.ДВ. 06 Дисциплины по выбору Блок 1.В.ДВ.6**

Дисциплина **«Психология и педагогика высшей школы» Б1.В. ДВ.06.01** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой прикладной психологии.

Дисциплина базируется на ранее изученных гуманитарных дисциплинах.

Дисциплина направлена на формирование следующих компетенций:

ОК-1: способность к абстрактному мышлению, анализу, синтезу;

ПК-11: способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности направления.

Содержание охватывает: психология и педагогика высшей школы как учебная дисциплина. Методологические основы психологии и педагогики высшей школы. Психолого-педагогические аспекты формирования и развития личности обучаемых в условиях высшей школы. Учебный коллектив как малая группа и объект педагогической деятельности преподавателя. Теория и практика организации и проведения учебного процесса в высшей школе. Психолого-педагогические аспекты воспитания обучаемых в условиях высшей школы. Педагогическая культура преподавателя, её формирование и развитие. Основы научно-исследовательской работы в высшей школе.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе во 2 семестре и предусматривает проведение учебных занятий следующих видов:

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

Программой предусмотрен итоговый контроль успеваемости в виде контрольной работы и зачета.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при освоении всех последующих дисциплин и выполнении выпускной квалификационной работы магистра.

Дисциплина **«Адаптированный коммуникативный практикум в профессиональной деятельности» Б1.В. ДВ.06.02** относится к вариативной части, дисциплины по выбору, блока 1 адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность»

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах адаптационного модуля бакалавриата вариативной части по выбору «Адаптивные информационные технологии», «Информационные технологии в профессиональной деятельности» и компетенциях: ОПК4 и ПК-1.

Дисциплина направлена на формирование следующих компетенций выпускника:

ОПК-2: способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности.

Содержание дисциплины охватывает круг вопросов, связанных с возможностями, особенностями и перспективами использования современных адаптивных информационных технологий в социальных науках, прогнозировании социальных процессов; основными подходами к применению информационных технологий при решении профессиональных задач социолога; ввод, обработка и анализ социологической информации.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, во 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся.

Программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольная работа, зачет.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

## **Блок 2. Практики, в том числе (НИР) Вариативная часть**

При определении мест прохождения практики обучающимися с ограниченными возможностями здоровья и инвалидами учитываются рекомендации, содержащиеся в заключении психолого-медико-педагогической комиссии, или рекомендации медико-социальной экспертизы, содержащиеся в индивидуальной программе реабилитации или

абилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для прохождения практики создаются специальные рабочие места в соответствии с характером ограничений здоровья, а также с учетом характера труда и выполняемых трудовых функций.

Формы проведения практики для инвалидов и лиц с ОВЗ могут быть установлены с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

При реализации данной программы предусматриваются следующие виды практик: производственная практика, педагогическая практика, практика по получению профессиональных умений и опыта профессиональной деятельности, научно-исследовательская работа (в том числе методология научного исследования), научно-исследовательская работа.

Практики направлены на формирование следующих компетенций выпускника:

#### **Б2.В.01 (П) Научно-исследовательская работа (в том числе методология научного исследования)**

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-1: способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности;

ПК-1: способность понимать и анализировать направления развития информационных (телекоммуникационных) технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способностью разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

ПК-13: способность организовать управление информационной безопасностью;

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

## **Б2.В.02 (П) Научно-исследовательская работа**

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок ;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

## **Б2.В.03 (П) Научно-исследовательская работа (в том числе методика написания диссертационной работы)**

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

## **Б2.В.04 (П) Педагогическая практика**

ОК-2: способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-2: способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности.

ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

## **Б2.В.05 (П) Практика по получению профессиональных умений и опыта профессиональной деятельности**

ПК-1: способность понимать и анализировать направления развития информационных (телекоммуникационных) технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-4: способность разработать программы и методики испытаний средств и систем обеспечения информационной безопасности.

ПК-5: способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества

ПК-6: способностью осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок

ПК-7: способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента

ПК-8: способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

ПК-11: способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности.

## **Б2.В.06 (П) Преддипломная практика**

ОК-1: способностью к абстрактному мышлению, анализу, синтезу;

ОК-2: способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

ОПК-1: способностью к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности;

ОПК-2: способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности;

ПК-1: способностью понимать и анализировать направления развития информационных (телекоммуникационных) технологий объекта защиты, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2: способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3: систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;



ПК-4: способностью разработать программы и методики испытаний средств и систем обеспечения информационной безопасности;

ПК-5: способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;

ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;

ПК-8: научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-11: способностью проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности.

Производственная, педагогическая и практика по получению профессиональных умений и опыта профессиональной деятельности, а также научно-исследовательская работа (в том числе методология научного исследования), научно-исследовательская работа являются обязательными разделами основной образовательной программы магистратуры и представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся.

Практики проводятся как на базе Университета, так и в сторонних организациях, обладающих необходимым кадровым и научно-техническим потенциалом.

Типы производственной практики: практика по получению профессиональных умений и опыта профессиональной деятельности; научно-исследовательская работа, педагогическая и преддипломная практика.

Педагогическая практика проводится для формирования у обучающихся профессиональных умений и опыта в преподавании дисциплин в области информационной безопасности.

Преддипломная практика проводится для выполнения магистерской диссертации и является обязательной.

Аттестация по итогам практики осуществляется на основе оценки решения обучающимися задач практики, отзыва руководителей практики об уровне его знаний и квалификации. По результатам аттестации выставляется дифференцированная оценка или зачет.

Программы практик, научно-исследовательской работы и государственной итоговой аттестации приведены в приложениях 3, 4, 5, 6, 7, 8, 9.

## **Факультативы**

### **Вариативная часть**

Факультативные дисциплины призваны углублять, расширять научные и прикладные знания обучающихся, 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 потребностями.

#### **ФТД.В.01 «Основы РЭБ в информационной безопасности»**

Дисциплина «Основы РЭБ в информационной безопасности» относится к факультативу адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах «Специальные разделы физики», «Специальные разделы математики», «Защищенные информационные системы», «Основы теории информационной безопасности» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,3,4,5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-14: способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК-16: способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

Содержание курса охватывает круг вопросов, связанных с изучением основ РЭБ в информационной безопасности: 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 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, во 2 семестре и предусматривает проведение учебных занятий следующих видов:

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

Программой предусмотрен итоговый контроль успеваемости в виде зачета во 2 семестре.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Технологии обеспечения информационной безопасности объектов», «Организационно-правовые механизмы обеспечения информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы магистра.

### **ФТД.В.02 «Организация спец проверок и спец исследований объектов информационной безопасности»**

Дисциплина «Организация спец проверок и спец исследований объектов информационной безопасности» относится к факультативу адаптированной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах «Специальные разделы физики», «Специальные разделы математики», «Защищенные информационные системы», «Основы теории информационной безопасности» и компетенциях: ОК-1,2, ОПК-1,2 и ПК-1,2,3,4,5,14.

Дисциплина направлена на формирование следующих компетенций выпускника:

ПК-8: способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-15: способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

Содержание курса охватывает круг вопросов, связанных с изучением основных принципов функционирования органов лицензирования и сертификации, испытательных центров, заявителей и их взаимодействие при проведении спец проверок и спец исследований объектов информационной безопасности. Изучается порядок проведения спец проверок и спец исследований (разработка заявки на проведение спец проверки и спец исследования, программы и методики сертификационных испытаний, их проведение), оформление и регистрация лицензии соответствия.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа. Преподавание дисциплины ведется на 1 курсе, во 2 семестре и предусматривает проведение учебных занятий следующих видов: лекции, практические занятия, самостоятельная работа обучающихся, групповые и индивидуальные консультации.

Программой предусмотрен итоговый контроль успеваемости в виде зачета во 2 семестре.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Технологии обеспечения информационной безопасности объектов», «Организационно-правовые механизмы обеспечения информационной безопасности», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы магистра.