ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДАЮ
Председатель СОП
д.т.н., доцент Аршинский Л.В.

_____
«25» мая 2018 г.
протокол № 6

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН И ПРАКТИК

ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ

НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.04.01 Информационная безопасность

ПРОФИЛЬ
Безопасность информационных систем и технологий

Квалификация выпускника – магистр
Форма и срок обучения – 2 года очная форма
Год начала подготовки – 2018
Общая трудоемкость – 120 з.е.
Выпускающая кафедра – «Информационные системы и защита информации»

ИРКУТСК 2018

Аннотация рабочей программы дисциплины
Б1.Б.01 «Деловой иностранный язык»

1 Цели и задачи освоения дисциплины «Деловой иностранный язык»

Цель освоения дисциплины:

− повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования, и овладение магистрантами необходимым и достаточным уровнем коммуникативной компетенции для решения социально-коммуникативных задач в области профессиональной и научной деятельности, а также для дальнейшего самообразования

Задачи освоения дисциплины:

− повышение уровня учебной автономии, способности к самообразованию;
− развитие когнитивных и исследовательских умений;
− развитие информационной культуры;
− расширение кругозора и повышение общей культуры магистрантов;
− воспитание толерантности и уважения к духовным ценностям разных стран и народов.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Деловой иностранный язык» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОК-1	способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности
ОК-3	способность свободно пользоваться русским и одним из иностранных языков как средством делового общения

В результате освоения дисциплины обучающийся должен:

знать:

− лексический минимум в объеме 500 учебных лексических единиц общего и терминологического характера;
− основные грамматические явления, характерные для профессиональной устной и письменной речи;
− правила речевого делового и профессионального этикета;
− основные правила письменного перевода текстов научного и делового стиля;

уметь:

− выразить свою точку зрения по актуальному вопросу, приводя необходимые пояснения и аргументы на иностранном языке;
− объяснить на иностранном языке суть проблемы и указать противоположной стороне в ходе дискуссии на преимущества и недостатки той или иной позиции;
− участвовать в диалоге на профессиональные темы с носителями изучаемого языка, не создавая препятствий языкового характера;
− сделать сообщение по теме научного исследования на иностранном языке;
− составить реферат и аннотацию научной статьи по специальности на иностранном языке;
− составить резюме, написать деловое письмо, сделать презентацию к докладу;
− понимать на слух сообщения на профессиональные темы;
− читать литературу по специальности на иностранном языке с целью общего понимания текста либо с целью извлечения необходимой информации;
− переводить литературу по специальности на иностранном языке, показывая полное и точное понимание профессиональной проблемы.

владеть:

− навыками использования официально-делового и научного стиля в письменной и устной формах;

− приемами аналитического чтения: отбора необходимой информации, умения отсекать малозначимую информацию, оценивать её важность и обобщать факты, понимания смысла текста, расшифровки истинной цели текста, адекватной реакции на прочитанное;

− приёмами самостоятельной и индивидуальной работы со справочными материалами, базами данных, компьютерными технологиями для формирования потребности к самообразованию, что подводит к необходимости самостоятельного изучения иностранного языка на протяжении всей жизни;

− навыками компьютерного перевода.

3 Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4 Содержание дисциплины

Раздел 1. Why do we choose magistracy course?

Раздел 2. The basics of translation.

Раздел 3. Business English.

Аннотация рабочей программы дисциплины
Б1.Б.02 «Современная философия и методология науки»

1 Цели и задачи освоения дисциплины «Современная философия и методология науки».

Цель освоения дисциплины:

– освоение общих закономерностей и конкретного многообразия форм функционирования науки в истории человеческой культуры и в системе философского знания.

Задачи освоения дисциплины:

– получение углубленных знаний в философии; формирование научного мировоззрения;

– создание комплексного представления о природе научного знания, структуре науки и ее месте в современной культуре, механизмах функционирования науки.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Современная философия и методология науки» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОК-1	способность совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

знать:

– особенности науки, ее место в культуре, нормативно-ценностную систему и этику науки;

– классификацию наук и научных исследований, основные особенности научного метода познания;

– основы философского понимания научных проблем;

– философско-методологические проблемы социально-гуманитарного знания;

– сущность философских проблем науки и техники;

уметь:

– применять методологию научного познания в профессиональной деятельности;

– анализировать логику рассуждений и высказываний;

– анализировать сущность философских проблем науки и техники;

владеть:

– способностью формировать представление о научной картине мира;

– философско-методологической основой исследований и разработок для решения поставленных профессиональных задач;

– навыками методологической рефлексии, анализа и интерпретации научных текстов, обзоров;

– способностью к обобщению, анализу, критическому осмыслению, систематизации, прогнозированию, постановке целей и выбору путей их достижения.

3 Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Предмет философии и методологии науки

Раздел 2 Основные этапы развития науки: преднаука и классическая наука.

Раздел 3 Неклассическая и постнеклассическая наука.

Раздел 4 Методологические проблемы и закономерности развития науки.

Раздел 5 Интеграция естественных, технических и гуманитарных наук.

Раздел 6 Единство чувственного и эмпирического познания.

Раздел 7 Теоретический уровень познания. Специфика и функции научной теории.

Раздел 8 Современная научная картина мира.

Раздел 9 Эволюция и революция в науке и технике.

Раздел 10 Типы научной рациональности. Стили научного мышления.

Аннотация рабочей программы дисциплины
Б1.Б.03 «Экономика и управление»

1 Цели и задачи освоения дисциплины «Экономика и управление».

Цель освоения дисциплины:

– формирование у обучающихся компетенций, необходимых для решения профессиональных задач в сфере информационной безопасности;

Задачи освоения дисциплины:

– привитие теоретических знаний и практических навыков анализа деятельности объекта экономической деятельности с целью выработки управленческих решений.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Экономика и управление» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-1	способность понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации
ПК-12	способность организовать работу коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ

В результате освоения дисциплины обучающийся должен:

знать:

– основы теории анализа микро- и макроэкономики;

– теорию экономического планирования и прогнозирования;

– методику оценки хозяйственной деятельности применительно к отрасли обеспечения информационной безопасности.

уметь:

– анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности;

– применять имеющиеся экономические знания в разработке управляющих решений на предприятии в условиях спектра мнений;

владеть:

– приемами экономического анализа и планирования;

– навыками организации работы коллектива в условиях спектра мнений.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Экономическая организация общества Сущность, типы и модели хозяйственных систем. Роль и место управления в хозяйственной системе. Функции государственного управления экономикой.

Раздел 2 Управление деятельностью хозяйствующих субъектов. Предприятие как основной хозяйствующий субъект. Классификация предприятий. Основные экономические стратегии фирмы. Структура управления фирмой и факторы ее определяющие. Планово-управленческая деятельность фирмы. Проблемы повышения эффективности использования факторов производства в деятельности хозяйствующих субъектов. Управление рисками как фактор устойчивого развития фирмы. Классификация рисков. Факторы риска. Управление рисками в механизме обеспечения экономической безопасности фирмы.

Раздел 3 Организационно-методические основы комплексного анализа хозяйственной деятельности. Особенности комплексного анализа как вида управленческой деятельности. Методика проведения комплексного анализа. Система показателей комплексного анализа. Методы и приемы комплексного анализа. Методы прогнозирования в экономическом анализе. Комплексный экономический анализ в разработке и обосновании бизнес-плана. Сметное планирование. Порядок формирования операционных, финансовых бюджетов, их основные показатели.

Раздел 4 Стратегический управленческий анализ производственной деятельности. Анализ производственно-хозяйственной деятельности. Анализ финансового состояния фирмы и его использование в управленческой деятельности.

Аннотация рабочей программы дисциплины
Б1.Б.04 «Защищенные информационные системы»

1 Цели и задачи освоения дисциплины «Защищенные информационные системы».

Цель освоения дисциплины:

– раскрыть основы нормативно-методическое регулирование процессов создания и эксплуатации защищенных информационных систем;

Задача освоения дисциплины:

– научить основам разработки безопасных продуктов и систем информационных технологий, а также методам противодействия угрозам информационной безопасности

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Защищенные информационные системы» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
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 разрабатывать программы и методики испытаний средств и систем 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

В результате освоения дисциплины обучающийся должен:

знать:

– понятие, виды и структуру автоматизированных систем;

– понятие и составляющие безопасности автоматизированных систем;

– схемы каталогизации угроз безопасности КС, способы их идентификации, спецификации и оценивания, роль человеческого фактора в угрозах безопасности ИС;

– понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности ИС;

– общую характеристику и методологию руководящих документов Гостехкомиссии/ФСТЭК по защите СВТ и АС от НСД к информации, классы защищенности и структуру функциональных требований к подсистемам защиты информации;

– общую характеристику и структуру стандартов по безопасности информационных технологий;

– виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИС;

– общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия;

– общую характеристику стандартов и особенности регламентации архитектуры систем защиты информации при взаимодействии открытых систем;

– модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления, оформления и утверждения Технического задания по созданию АС, состав и структуру основных документов;

– особенности создания защищенных ИС;

– модель жизненного цикла и порядок создания изделий ИС, удовлетворяющих требованиям безопасности, способы задания требований безопасности, структуру, порядок разработки, оценки, утверждения и опубликования профилей защиты изделий ИТ, заданий по безопасности при создании ИС;

– основы методов и технологий проектирования защищенных компьютерных систем;

– основы управления проектированием ИС;

– основы планирования и графического представления процессов;

– общие положения по эксплуатации ИС;

– содержание процессов администрирования и эксплуатации ИС.

уметь:

– идентифицировать и оценивать угрозы безопасности при формировании требований пользователя к ИС;

– определять и оформлять класс защищенности создаваемой ИС;

– составлять и правильно оформлять основные разделы Технического задания на создание несложных ИС (системы защиты информации ИС);

– составлять отдельные разделы Профиля защиты применительно к простым видам ИС;

– планировать индивидуально-групповою структуру пользователей ИС и структуру разделяемых (коллективных) информационных ресурсов;

– разрабатывать политику безопасности и регламентации работы с ИС;

– понимать, как генерировать, хранить и эксплуатировать парольные и другие средств аутентификации пользователей ИС;

– хранение информационных ресурсов, эксплуатации сменных носителей информации;

– разрабатывать структуру и отдельные разделы Руководства пользователя;

– исполнять обязанности администратора ИС.

владеть:

– навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты информации в ИС и внедрять их в практику;

– навыками внедрения средств защиты.

3 Общая трудоемкость дисциплины составляет 4 зачетных единицы или 144 часа.

4 Содержание дисциплины

Раздел 1 Понятие, виды и структура информационных систем. Понятие защищенной ИС.

Раздел 2 Объекты защиты и угрозы безопасности в информационных системах.

Раздел 3 Методы защиты от основных видов угроз и перекрытие уязвимостей.

Раздел 4 Жизненный цикл и порядок создания защищенных ИС.

Раздел 5 Основы методов и технологий проектирования защищенных информационных систем.

Раздел 6 Администрирование и эксплуатация защищенных ИС.

Раздел 7 Политика безопасности и основные требования к ее построению.

Раздел 8 Анализ и построение защиты локальных внутренних и распределенных внешних вычислительных и информационных сетей предприятия.

Раздел 9 Анализ среды предприятия с точки зрения информационной безопасности, выявление ключевых элементов и оценка их влияние на предприятие. Оперативные задачи реализации защиты данных, информации, информационных и вычислительных систем во всех подразделениях предприятия.

Раздел 10 Разработка конкретных мер по обеспечению корпоративной информационной безопасности с учетом конкурентной ситуации и стратегии развития организации.

Аннотация рабочей программы дисциплины
Б1.Б.05 «Управление информационной безопасностью»

1 Цели и задачи освоения дисциплины «Управление информационной безопасностью».

Цель освоения дисциплины:

– изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задача освоения дисциплины:

– овладение основными понятиями, методологией и практическими приемами управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Управление информационной безопасностью» направлено на формирование компетенций

Код компетенции	Содержание компетенции
ПК-13	способность организовать управление информационной безопасностью
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения

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

В результате освоения дисциплины обучающийся должен:

знать:

- основные методы управления информационной безопасностью;
- методы аттестации уровня защищенности информационных систем;
- основные угрозы безопасности информации и модели нарушителя в информационных системах;
- принципы формирования политики информационной безопасности в информационных системах.

уметь:

- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем;
- выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем;
- оценивать информационные риски в информационных системах;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;
- разрабатывать частные политики информационной безопасности информационных систем;
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем.

владеть:

- навыками анализа информационной инфраструктуры информационной системы и ее безопасности;
- методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
- методами управления информационной безопасностью информационных систем;
- методами оценки информационных рисков;
- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем;
- навыками участия в экспертизе состояния защищенности информации на объекте защиты.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Система управления информационной безопасностью.

Раздел 2 Комплексная система защиты информации.

Раздел 3 Управление комплексной системой защиты информации.

Аннотация рабочей программы дисциплины

Б1.Б.06 «Технологии обеспечения информационной безопасности объектов»

1 Цели и задачи освоения дисциплины «Технологии обеспечения информационной безопасности объектов».

Цель освоения дисциплины:

– является формирование у обучающихся твёрдых знаний и умений по раскрытию сущности и значения технологии обеспечения информационной безопасности объектов с умением анализировать угрозы информационной безопасности и планировать эффективные меры по обеспечению информационной безопасности на объектах;

– является изучение методов и средств обеспечения информационной безопасности, создания и эксплуатации защищенных информационных сетей

Задачи освоения дисциплины:

– изучение методов и средств обеспечения информационной безопасности, создания и эксплуатации защищенных информационных сетей

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Технологии обеспечения информационной безопасности объектов» направлено на формирование компетенций.

Код компетенции	Содержание компетенции
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
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

В результате освоения дисциплины обучающийся должен:

знать:

– понятие, виды и структуру автоматизированных систем;

– понятие и составляющие безопасности автоматизированных систем;

– схемы каталогизации угроз безопасности КС, способы их идентификации;

– спецификации и оценивания, роль человеческого фактора в угрозах безопасности ИС;

– понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности ИС;

– общую характеристику и методологию руководящих документов Гостехкомиссии/ФСТЭК по защите СВТ и АС от НСД к информации, классы защищенности и структуру функциональных требований к подсистемам защиты информации;

– общую характеристику и структуру стандартов по безопасности информационных технологий;

– виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИС;

– общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия;

– общую характеристику стандартов и особенности регламентации архитектуры систем защиты информации при взаимодействии открытых систем;

– модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления,

оформления и утверждения Технического задания по созданию АС, состав и структуру основных документов;

– особенности создания защищенных ИС;

– модель жизненного цикла и порядок создания изделий ИС, удовлетворяющих требованиям безопасности, способы задания требований безопасности, структуру, порядок разработки, оценки, утверждения и опубликования профилей защиты изделий ИТ, заданий по безопасности при создании ИС;

– основы методов и технологий проектирования защищенных компьютерных систем;

– основы управления проектированием ИС;

– основы планирования и графического представления процессов;

– общие положения по эксплуатации ИС;

– содержание процессов администрирования и эксплуатации ИС;

уметь:

– идентифицировать и оценивать угрозы безопасности при формировании требований пользователя к ИС;

– определять и оформлять класс защищенности создаваемой ИС;

– составлять и правильно оформлять основные разделы Технического задания на создание несложных ИС (системы защиты информации ИС);

– составлять отдельные разделы Профиля защиты применительно к простым видам ИС;

– составлять диаграммы Гантта и сетевые графики несложных процессов проектирования, осуществлять их анализ и оптимизацию;

– планировать индивидуально-групповою структуру пользователей ИС и структуру разделяемых (коллективных) информационных ресурсов;

– разрабатывать политику безопасности и регламентации работы с ИС;

– понимать, как генерировать, хранить и эксплуатировать парольных и других средств аутентификации пользователей ИС;

– хранение информационных ресурсов, эксплуатации сменных носителей информации;

– разрабатывать структуру и отдельные разделы Руководства пользователя;

– исполнять обязанности администратора ИС;

владеть:

– навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты информации в ИС и внедрять их в практику;

– навыками внедрения средств защиты.

3 Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

4 Содержание дисциплины

Раздел 1 Информационные системы.

Раздел 2 Угрозы безопасности ИС.

Раздел 3 Методы защиты ИС.

Раздел 4 Жизненный цикл ИС.

Раздел 5 Методы проектирования защищенных ИС. Нормативно-правовая база.

Раздел 6 Эксплуатация защищенных ИС.

Раздел 7 Документальное оформление к безопасности ИС.

Аннотация рабочей программы дисциплины
Б1.В.01 «Специальные разделы математики»

1 Цели и задачи освоения дисциплины «Специальные разделы математики.

Цель освоения дисциплины:

– ознакомление обучающихся со специальным математическим инструментарием, необходимым для решения профессиональных задач в сфере информационной безопасности.

Задачи освоения дисциплины:

– овладение обучающимися специальным математическим инструментарием, необходимым для решения профессиональных задач в сфере информационной безопасности.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Специальные разделы математики» направлено на формирование компетенций.

Код компетенции	Содержание компетенции
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

В результате освоения дисциплины обучающийся должен:

знать:

– основные типы статистических задач и математические методы их решения;

– основные математические методы исследования случайных процессов;

– основные теоретико-числовые методы применительно к задачам защиты информации;

уметь:

− самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученных моделей и реальных задач;

− применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации;

владеть:

– навыками аналитического и численного решения задач математической статистики; расчета и оценки криптографических систем.

3 Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

4 Содержание дисциплины

Раздел 1 Теория случайных процессов

Раздел 2 Математические основы защиты информации в приложении к криптографии.

Аннотация рабочей программы дисциплины
Б1.В.02 «Специальные разделы физики»

1 Цели и задачи освоения дисциплины «Специальные разделы физики»

Цель освоения дисциплины:

– получение знаний об основных физических принципах, использующихся при реализации технических каналов утечки информации, а также при разработке и функционировании систем защиты информации;

Задачи освоения дисциплины:

– изучение основных физических законов и принципов, использующихся при реализации технических каналов утечки информации (ТКУИ) и методов защиты информации. Привитие навыков анализа физических процессов и явлений при реализации ТКУИ.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Специальные разделы физики» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
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

В результате освоения дисциплины обучающийся должен:

знать:

− основные физические принципы реализации технических каналов утечки информации и построения систем защиты информации;

− демаскирующие признаки сигналов;

− особенности воздействия шумов и помех на радиотехнические системы в различных диапазонах длин волн;

− принципы работы радиотехнических систем;

уметь:

− выявлять возможные технические каналы утечки информации на основе анализа их физических принципов, осуществлять выбор технических средств защиты нейтрализующих угрозы безопасности информации;

владеть:

− навыками работы с контрольно-измерительной аппаратурой при выявлении технических каналов утечки информации.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Основные элементы канала реализации угроз безопасности информации.

Раздел 2 Краткие сведения по акустике.

Раздел 3 Демаскирующие признаки сигналов.

Раздел 4 Особенности распространения радиоволн различных диапазонов.

Раздел 5 Основные характеристики оптического и лазерного излучений.

Раздел 6 Радиотехнические системы передачи информации.

Аннотация рабочей программы дисциплины
Б1.В.03 «Математическое моделирование технических объектов и систем управления»

1 Цели и задачи освоения дисциплины «Математическое моделирование технических объектов и систем управления».

Цель освоения дисциплины:

– является получение углубленных знаний в области анализа и математического моделирования объектов технической природы и систем управления различной функциональной направленности.

Задачи освоения дисциплины:

– овладение методами математического моделирования объектов технической природы и систем управления различной функциональной направленности

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Математическое моделирование технических объектов и систем управления» направлено на формирование компетенций

Код компетенции	Содержание компетенции
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

В результате освоения дисциплины обучающийся должен:

знать:

− методики построения комплексных систем математических моделей объектов различной природы;

уметь:

− оценивать адекватность моделей и интерпретировать результаты моделирования и прогнозирования;

владеть:

− современными компьютерными технологиями моделирования и навыками создания соответствующих программных средств.

3 Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 часов.

4 Содержание дисциплины

Раздел 1 Понятие модели. Классификация моделей. Этапы моделирования.

Раздел 2 Методы идентификации параметров модели.

Раздел 3 Проблема верификации моделей.

Раздел 4 Динамические модели. Экспертно-статистические модели.

Раздел 5 Прогнозирование по статистическим моделям.

Аннотация рабочей программы дисциплины
Б1.В.04 «Теория игр и исследование операций»

1 Цель освоения дисциплины «Теория игр и исследование операций»

Цель освоения дисциплины:

– научить математическому моделированию конфликтных ситуаций и формированию математических методов и алгоритмов поиска оптимальных стратегий

Задача освоения дисциплины:

– овладение методами математического моделирования конфликтных ситуаций и поиска оптимальных стратегий.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Теория игр и исследование операций» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-6	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества

ПК-7	способность анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им

В результате освоения дисциплины обучающийся должен:

знать:

– основные задачи, при решении которых возникает необходимость использования математических методов теории игр и исследования операций;

– основные понятия теории игр и исследования операций;

– ориентироваться в каком разделе теории игр и исследования операций следует искать средства решения задач теории игр и исследования операций;

уметь:

– формализовать задачу теории игр и исследования операций и описать ее с помощью известных математических моделей;

– проанализировать полученные результаты и сделать выводы по поставленной задаче;

– проводить расчеты, получать количественные результаты;

владеть:

– основными методами принятия решений в условиях риска и неопределенности;

– аналитическими и графическими методами решения задач теории игр и исследования операций.

3 Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Введение. Модели исследования операций. Линейное программирование. Транспортные задачи.

Раздел 2 Основные понятия теории игр. Стратегии, ситуации, функции выигрыша. Принципы оптимальности.

Раздел 3 Антагонистические (матричные) игры. Ситуации равновесия. Седловая точка. Решение игры.

Раздел 4 Игры с природой.

Раздел 5 Биматричные игры.

Раздел 6 Игры многих лиц с непротивоположными интересами.

Аннотация рабочей программы дисциплины
Б1.В.05 «Теоретические основы управления»

1 Цели и задачи освоения дисциплины «Теоретические основы управления».

Цели освоения дисциплины:

– освоение магистром понятийного аппарата управления;

– выработка целостного восприятия системы управления.

Задача освоения дисциплины:

– освоение методов организационного проектирования и организационно-управленческого анализа, приемов и методов управленческой деятельности.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Теоретические основы управления» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-12	способность организовать выполнение работ, управлять коллективом исполнителей и принимать управленческие решения
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

В результате освоения дисциплины обучающийся должен:

знать:

– порядок выполнения работ коллектива;

– мероприятия по реализации проектов и программ.

уметь:

– определять порядок выполнения работ;

– составлять план мероприятий по реализации разработанных проектов и программ.

владеть:

– способами определения порядка выполнения работ;

– методами планирования осуществления проектов и программ.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Концепции управления.

Раздел 2 Связующие функции управления предприятиями, проектами и программами.

Раздел 3 Теоретические основы власти и руководства.

Раздел 4 Основы целеполагания и планирования объектов управления.

Раздел 5 Теоретические основы целевых функций управления.

Раздел 6 Теоретические основы организационной функции управления.

Раздел 7 Теоретические основы функций лидерства в управлении.

Раздел 8 Теоретические основы мотивационной функции управления.

Раздел 9 Теории эффективности управления социальными системами.

Аннотация рабочей программы дисциплины
Б1.В.06 «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем»

1 Цели и задачи освоения дисциплины «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем».

Цели освоения дисциплины:

– получение углубленных знаний в сфере технологии экспертных систем (ЭС);

– получение знаний в области применения технологии ЭС для решения проблем информационной безопасности (ИБ);

– формирование компетенций в области моделирования предметных областей ИБ с помощью знаний;

– овладение основами фундаментальных знаний в области теории ЭС;

– формирование представления об основных задачах ИБ, решаемых средствами ЭС; формирование представления о тенденциях развития данного направления в России и за рубежом.

Задача освоения дисциплины:

– теоретическое и практическое освоение методов разработки эффективных систем управления информационной безопасностью

3 Требования к результатам освоения дисциплины

Освоение дисциплины «Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки

ПК-13	способность организовать управление информационной безопасностью

В результате освоения дисциплины обучающийся должен:

знать:

– базовые положения теории ЭС;

– задачи ИБ, решаемые средствами ЭС;

– классические модели знаний и рассуждений;

– модели правдоподобных рассуждений;

– инструментальные средства разработки ЭС;

– особенности применения ЭС в ИБ.

уметь:

– выявлять задачи ИБ, решаемые на основе технологий ЭС;

– решать поставленные задачи с помощью соответствующих инструментальных средств;

владеть:

– основными концепциями моделирования предметных областей на основе технологии ЭС;

– инструментальными и языковыми средствами решения задач ИБ с помощью ЭС.

3 Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

4 Содержание дисциплины

Раздел 1 Основы экспертных систем.

Раздел 2 Моделирование знаний.

Раздел 3 Моделирование рассуждений.

Раздел 4 Инструментальные средства разработки экспертных систем.

Аннотация рабочей программы дисциплины
Б1.В.07 «Организационно-правовые механизмы обеспечения информационной безопасности»

1 Цели и задачи освоения дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности».

Цель освоения дисциплины:

– изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационно - правового обеспечения информационной безопасности и защиты информации.

Задача освоения дисциплины:

– формирование представлений о теоретических, методологических и практических проблемах формирования, функционирования и развития систем организационно - правового обеспечения информационной безопасности и защиты информации.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» направлено на формирование компетенций

Код компетенции	Содержание компетенции
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-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен:

знать:

- основные методы управления информационной безопасностью;
- методы аттестации уровня защищенности информационных систем;
- основные угрозы безопасности информации и модели нарушителя в информационных системах;
- принципы формирования политики информационной безопасности в информационных системах;
- основные положения государственной политики обеспечения информационной безопасности;
- критерии, условия и принципы отнесения информации к защищаемой;

уметь:

- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем;
- выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем;
- оценивать информационные риски в информационных системах;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем;
- разрабатывать частные политики информационной безопасности информационных систем;
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем.

владеть:

- навыками анализа информационной инфраструктуры информационной системы и ее безопасности;
- методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем;
- методами управления информационной безопасностью информационных систем;
- методами оценки информационных рисков;
- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем;
- навыками участия в экспертизе состояния защищенности информации на объекте защиты.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Правовые механизмы обеспечение информационной безопасности.

Раздел 2 Организационные механизмы обеспечение информационной безопасности.

Аннотация рабочей программы дисциплины
Б1.В.08 «Методы и средства защиты информации в системах электронного документооборота»

1 Цели и задачи освоения дисциплины «Методы и средства защиты информации в системах электронного документооборота.

Цель освоения дисциплины:

– является формирование у обучающихся твёрдых знаний и умений по раскрытию сущности и значения технологии защищённого документооборота в условиях применения различных типов носителей документированной информации, а также различных методов и средств в системах конфиденциального документооборота;

– является изучение методов защиты информации, выявления угроз информационной безопасности и построения эффективной системы защиты в системах электронного документооборота.

Задача освоения дисциплины:

– изучение методов защиты информации, выявления угроз информационной безопасности и построения эффективной системы защиты в системах электронного документооборота.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Методы и средства защиты информации в системах электронного документооборота» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
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-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

В результате освоения дисциплины обучающийся должен:

знать:

– теоретические и методические основы рационального построения защищенного документооборота в любых организационных структурах;

– функциональные возможности и предпосылки эффективного применения различных типов технологических систем и способов обработки и хранения конфиденциальных документов;

– принципы и методы обработки конфиденциальных документов в потоках при любых используемых типах систем и способах выполнения процедур и операций по обработке и хранению этих документов;

– методы и приемы защиты документированной информации и носителя этой информации от несанкционированного доступа в процессе выполнения каждой процедуры и операции;

– порядок обработки, движения, хранения и использования конфиденциальных документов в ведомственных архивах;

– организацию работы руководителей, специалистов и технического персонала с конфиденциальными документами на любом носителе информации;

уметь:

– разрабатывать и оформлять нормативно-методические материалы по регламентации процессов обработки, хранения и защиты конфиденциальных документов;

– разрабатывать эффективные технологические схемы рационального документооборота с использованием современных систем и способов обработки и хранения конфиденциальных документов;

– формулировать задачи по разработке потребительских требований к автоматизированным системам обработки и хранения конфиденциальных документов;

– разрабатывать и совершенствовать внемашинную часть организации и технологии функционирования автоматизированных систем обработки и хранения конфиденциальных документов;

– практически выполнять технологические операции по защите и обработке конфиденциальных документов в организационных структурах;

– руководить службой конфиденциальной документации;

– контролировать и анализировать уровень организационной и технологической защищенности документов;

владеть:

– основами информационной безопасности и защиты информации;

– специальной профессиональной терминологией;

– основными элементами защиты и обработки конфиденциальных документов.

3 Общая трудоемкость дисциплины составляет 3 зачетных единицы, 144 часа.

4 Содержание дисциплины

Раздел 1 Бумажный конфиденциальный документооборот.

Раздел 2 Электронный конфиденциальный документооборот.

Аннотация рабочей программы дисциплины
Б1.В.09 «Теория систем и системный анализ»

1 Цель освоения дисциплины «Теория систем и системный анализ».

Цель освоения дисциплины:

– изучение новых подходов качественной теории систем, базирующейся на системном анализе состояния прикладных информационных технологий, закономерностей функционирования и развития систем, методов и моделей теории систем.

Задача освоения дисциплины:

– сформировать представление о методах и подхода качественной теории систем.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Теория систем и системный анализ» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОК-1	способность к абстрактному мышлению, анализу, синтезу
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

В результате освоения дисциплины обучающийся должен:

знать:

– основные принципы системных исследований, методики моделирования сложных систем;

– основные тенденции развития системного анализа, принятия решений и управления в различных областях науки и техники;

уметь:

– ставить проблему комплексного исследования объекта на основе применения методологии системного анализа;

– разрабатывать математические модели технических и социально-экономических объектов;

владеть:

– современными методами системного анализа объектов и процессов;

– основными приемами формализации содержательных задач;

– средствами информационных технологий и способами их применения для решения задач системного анализа в различных предметных областях.

3 Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

4 Содержание дисциплины

Раздел 1 Система как объект исследования.

Раздел 2 Этапы реализации методологии системного анализа для решения проблем.

Раздел 3 Математическое моделирование как один из основных этапов методологии системного анализа.

Раздел 4 Применение методологии системного анализа для решения практических задач.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.01.01 «Интеллектуальные информационные системы»

1 Цели и задачи освоения дисциплины «Интеллектуальные информационные системы»

Цели освоения дисциплины:

– получение углубленных знаний и формирование компетенций в области методологических и прикладных вопросов теории искусственного интеллекта (ИИ),

– получение фундаментальных знаний о принципах и основах применения интеллектуальных информационных систем (ИИС) в сфере информационной безопасности.

Задача освоения дисциплины:

– формирование представлений об особенностях использования технологий ИИ в сфере защиты информации, о тенденциях развития данного направления в России и за рубежом. Привитие навыков работы с системами ИИ в сфере ИБ.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Интеллектуальные информационные системы» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества

В результате освоения дисциплины обучающийся должен:

знать:

− теорию и фундаментальные основы технологий искусственного интеллекта, в т.ч. применительно к проблеме информационной безопасности;

уметь:

− решать прикладные вопросы разработки и эксплуатации интеллектуальных систем, в т.ч. применительно к задачам информационной безопасности;

владеть:

− методами и инструментальными средствами разработки и эксплуатации систем искусственного интеллекта, в т.ч. в сфере защиты информации.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Введение в дисциплину.

Раздел 2 Экспертные системы.

Раздел 3 Распознавание образов.

Раздел 4 Нейронные сети.

Раздел 5 Искусственный интеллект проблемах информационной безопасности.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.01.02 «Корпоративные информационные системы»

1 Цели и задачи освоения дисциплины «Корпоративные информационные системы».

Цели освоения дисциплины:

- выявление особенностей построения корпоративных информационных систем;
- изучение устройства корпоративных информационных систем и области их применения, современных технологий автоматизации производства и управления, существующих аппаратно-программных платформ, интерфейсов и межсетевых протоколов;
- изучение основных принципов проектирования и программирования корпоративных информационных систем.

Задача освоения дисциплины:

- овладение принципами разработки и функционирования корпоративных информационных систем

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Корпоративные информационные системы» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной

В результате освоения дисциплины обучающийся должен:

знать:

- экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отраслям обеспечения информационной безопасности);
- информационные технологии управления корпорациями;
- аппаратные и программные средства обеспечения сетевого взаимодействия компонентов информационных систем;
- средства моделирования информационных систем;
- средства быстрой разработки информационных систем;

уметь:

- анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности;
- создавать проекты информационных систем;
- применять информационные технологии при разработке информационных систем предприятий;
- создавать средства интерфейса пользователя;

владеть:

- приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям;
- навыками выбора аппаратно-программной платформы ИС;
- средствами обеспечения сетевого взаимодействия компонентов информационных систем;
- принципами построения локальных и глобальных связей;
- средствами межсетевого взаимодействия.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Введение.

Раздел 2 Корпоративные информационные системы (КИС).
Раздел 3 Проектирование, разработка и функционирование КИС.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.02.01 «Проектирование информационных систем»

1 Цель освоения дисциплины «Проектирование информационных систем»

Цель освоения дисциплины:

− получение углубленных знаний и формирование компетенций в области методологических и прикладных вопросов проектирования информационных систем, принципов и основ создания и использования информационных систем в сфере информационной безопасности.

Задача освоения дисциплины:

− овладение навыками в области принципов и основ создания и использования информационных систем в сфере информационной безопасности.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Проектирование информационных систем» направлено на формирование компетенций

Код компетенции	Содержание компетенции
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, 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

В результате освоения дисциплины обучающийся должен:

знать:

− основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;

− методы концептуального проектирования технологий обеспечения информационной безопасности;

уметь:

− осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;

− обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;

владеть:

− навыками управления информационной безопасностью простых объектов.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Информационные системы и способы их внедрения.
Раздел 2 Модели жизненного цикла ИС. Стандарты разработки ИС.
Раздел 3 Технологии проектирования ИС. CASE-средства.
Раздел 4 Методологии проектирования ИС, ориентированные на модель ЖЦ ИС.
Раздел 5 Проектирование баз данных и хранилищ данных.
Раздел 6 Проект. Управление проектом. Средства управления проектом.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.02.02 «Структуры и алгоритмы обработки данных»

1 Цели и задачи освоения дисциплины «Структуры и алгоритмы обработки данных».

Цель освоения дисциплины:

– формирование важнейших представлений о структурах данных и алгоритмах их обработки в информационных системах.

Задача освоения дисциплины:

– передача обучаемым теоретических основ по алгоритмам обработки информации, включая вопросы поиска, сортировки, сжатия, решения прикладных задач на графах и других с учетом развития информационных технологий и систем.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Структуры и алгоритмы обработки данных» направлено на формирование компетенций:

Код компетенции	Название компетенции
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности
ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента

В результате изучения дисциплины обучающийся должен:

знать:

– основные сведения о дискретных структурах, используемых в персональных компьютерах;

– основные алгоритмы типовых методов решения задач.

уметь:

– осуществлять математическую и информационную постановку задач по обработке информации, использовать алгоритмы обработки информации для различных приложений.

владеть:

– практическими навыками программной реализации алгоритмов обработки данных.

3 Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Простые методы сортировки. Оценки сложности алгоритма.

Раздел 2 Усовершенствованные алгоритмы сортировки. Сортировка Шелла.

Раздел 3 Быстрая сортировка методом разделения Хоара.

Раздел 4 Поиск вхождения слова в текст. Алгоритм Боуэра-Мура.

Раздел 5 Алгоритм Кнута-Мориса-Пратта.

Раздел 6 Алгоритм построения минимального остовного дерева.

Раздел 7 Алгоритм поиска кратчайшего пути

Раздел 8 Алгоритмы распознавания образов на основе функций расстояния.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.03.01 «Инструментарий анализа информационных рисков»

1 Цели и задачи освоения дисциплины «Инструментарий анализа информационных рисков».

Цель освоения дисциплины:

– раскрытие сущности и значения инструментария анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации, определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации;

– определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;

– оценить существующие методические подходы и инструментарий в оценке информационных рисков для выявления возможностей совершенствования данной деятельности;

– изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта;

– освоить методические положения и инструментарий в совершенствовании деятельности в сфере оценки информационных рисков хозяйствующих субъектов;

– освоить методические подходы и инструментарий в оценке эффективности деятельности по защите информационных активов предприятия.

Задачи освоения дисциплины:

– определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;

– оценить существующие методические подходы и инструментарий в оценке информационных рисков для выявления возможностей совершенствования данной деятельности;

– изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта;

– освоить методические положения и инструментарий в совершенствовании деятельности в сфере оценки информационных рисков хозяйствующих субъектов; освоить методические подходы и инструментарий в оценке эффективности деятельности по защите информационных активов предприятия.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Инструментарий анализа информационных рисков» направлено на формирование компетенций

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

В результате освоения дисциплины обучающийся должен:

знать:

– роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;

– существующие методические подходы и инструментарий в оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов;

– особенности и проблемы организационного направления в деятельности по защите информационных активов;

– методический подход и инструментарий в оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков;

– основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия;

уметь:

– выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты;

– определять состав, важность и ценность конфиденциальной информации применительно к видам тайны;

– выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;

– выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;

– определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия;

– организовывать системное обеспечение защиты информации;

владеть:

– основами информационной безопасности и защиты информации;

– специальной профессиональной терминологией;

– основными элементами и инструментарием по выявлению информационных рисков реализации угроз конфиденциальной информации.

3 Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов.

4 Содержание дисциплины

Раздел 1 Теоретические подходы к анализу информационных рисков.

Раздел 2 Практика и технология анализа информационных рисков на предприятии.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.03.02 «Виртуальные частные сети»

1 Цели и задачи освоения дисциплины «Виртуальные частные сети»

Цель освоения дисциплины:

– изучение технологий, методов и средств обеспечения безопасного информационного обмена на базе построения виртуальных частных сетей (VPN) для использования в распределенных корпоративных сетях (РКС) предприятий, организаций и учреждений.

Задача освоения дисциплины:

– ознакомить обучающихся с технологиями, методами и средствами обеспечения безопасного информационного обмена на базе построения виртуальных частных сетей (VPN) для использования в распределенных корпоративных сетях (РКС) предприятий, организаций и учреждений

2 Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Виртуальные частные сети» направлен на формирование следующих компетенций:

Код компетенции	Наименование компетенции
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности

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

В результате изучения дисциплины обучающийся должен:

знать:

– методы концептуального проектирования технологий обеспечения защищенного информационного обмена;

– классификацию VPN;

– уровни реализации и структуру VPN;

– функции и возможности стандартных и специализированных средств построения VPN;

уметь:

– находить решение по выбору необходимого уровня защиты информационного обмена в зависимости от требований политики безопасности предприятия/организации;

– проводить выбор средств построения VPN для использования их в составе РКС с целью обеспечения требуемого уровня защищенности;

– создавать необходимые условия использования средств построения;

– экономически эффективно использовать программно-аппаратные средства обеспечения ИБ технологий в профессиональной деятельности;

– применять в различных проектах средства построения VPN;

владеть:

– навыками использования различных видов/типов средств организации VPN.

3 Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 час.

4 Содержание дисциплины

Раздел 1 Виртуальная частная сеть как средство защиты информации.

Раздел 2 Стандартные протоколы создания виртуальных частных сетей.

Раздел 3 Управление криптографическими ключами в виртуальных частных сетях.

Раздел 4 Построение виртуальной частной сети.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.04.01 «Программно-аппаратные средства защиты информации. Дополнительные главы»

1 Цель освоения дисциплины «Программно-аппаратные средства защиты информации. Дополнительные главы»:

Цель освоения дисциплины:

– получение знаний о назначении, функциях и возможностях добавочных программно-аппаратных средств защиты информации (ПАСЗИ), а также соответствующих навыков
их администрирования.

Задача освоения дисциплины:

– освоение добавочных ПАСЗИ.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Программно-аппаратные средства защиты информации. Дополнительные главы» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
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-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

знать:

– состав компонент и функции добавочных ПАСЗИ от несанкционированного доступа (НСД);

– возможности и способы использования безопасных информационных технологий при практической эксплуатации ПАСЗИ;

уметь:

– проводить выбор ПАСЗИ с целью обеспечения требуемого уровня защищенности;

– применять в различных проектах программно-аппаратные средства обеспечения информационной безопасности;

– администрировать ПАСЗИ;

владеть:

– навыками применения ПАСЗИ (на основе программно-технических и программных образцов).

3 Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4 Содержание дисциплины

Раздел 1 Система защиты информации (СЗИ) от НСД Secret Net.

Раздел 2 СЗИ Secret Net Studio.

Раздел 3 Средство защиты информации vGate.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.04.02 «Криптографические протоколы»

1 Цель освоения дисциплины «Криптографические протоколы»:

Цель освоения дисциплины:

– изучение криптографических протоколов, методов их анализа, основных сфер практического применения и особенностей реализации.

Задача освоения дисциплины:

– освоить криптографические протоколы, и методы их анализа

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Криптографические протоколы» направлено на формирование компетенций:

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

В результате освоения дисциплины обучающийся должен:

знать:

– основные классы криптографических протоколов;

– виды атак на криптопротоколы;

– принципы анализа криптографических протоколов;

уметь:

– оценивать функциональные возможности криптопротоколов;

– производить обоснованный выбор средств защиты информации на основе криптографических протоколов;

владеть:

– навыками анализа российских и международных стандартов по идентификации и аутентификации субъектов;

– навыками анализа уязвимостей криптографических протоколов.

3 Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4 Содержание дисциплины

Раздел 1 Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов.

Раздел 2 Классификация криптографических протоколов. Атаки на криптопротоколы.

Раздел 3 Формальные методы анализа протоколов обеспечения безопасности.

Раздел 4 Протоколы идентификации и аутентификации. Протоколы, использующие технику доказательства знания. Игровые протоколы.

Раздел 5 Протоколы передачи ключей.

Раздел 6 Протокол TLS/SSL.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.05.01 «Защита в государственных информационных системах»

1 Цели и задачи освоения дисциплины «Защита в государственных информационных системах».

Цель освоения дисциплины:

– получение знаний и навыков в области реализации системы защиты информации в государственных информационных системах;

Задача освоения дисциплины:

– изучение законодательных и иных нормативных актов по функционированию и защите ГИС, а так же получение навыков разработки системы защиты ИС.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Защита в государственных информационных системах» направлено на формирование компетенций

Код компетенции	Содержание компетенции
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

В результате освоения дисциплины обучающийся должен:

знать:

– основные нормативно-правовые и организационно-распорядительные документы в области защиты государственных информационных систем;

– основные требования к защите информации, содержащейся в государственной информационной системе;

– порядок аттестации государственных информационных систем;

– особенности защиты информации в отдельных государственных информационных системах;

уметь:

– разрабатывать необходимые организационно-распорядительные документы по защите информации в государственных информационных системах;

– определять класс защищенности государственной информационной системы;

– формировать требования к защите информации, содержащейся в государственной информационной системе;

владеть:

– навыками работы со средствами защиты информации от несанкционированного доступа и средствами криптографической защиты информации.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Государственные информационные системы.

Раздел 2 Защита информации в государственных информационных системах.

Раздел 3 Особенности защиты государственных информационных систем.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.05.02 «Методология определения ценности информации»

1 Цели и задачи освоения дисциплины «Методология определения ценности информации».

Цель освоения дисциплины:

– раскрытие значения ценности информации для субъектов информационных отношений (личности, общества, государства), роли защиты информации в обеспечении прав граждан, ее места в политической, экономической, военной и других областях деятельности, в безопасности функционирования различных хозяйственных и управленческих структур.

Задачи освоения дисциплины:

– сформировать представление о ценности информации для различных субъектов, роли защиты информации в обеспечении прав граждан, безопасности функционирования хозяйственных и управленческих структур

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Методология определения ценности информации» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, 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

В результате освоения дисциплины обучающийся должен:

знать:

– базовый понятийный аппарат в области экономических методов защиты информации;

– виды и состав угроз в экономике защиты информации;

– методы выявления рисков реализации угроз информационной безопасности;

– принципы и общие методы определения ценности информации;

– основные положения государственной политики обеспечения информационной безопасности;

– критерии, условия и принципы отнесения информации к защищаемой

– виды носителей защищаемой информации;

– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;

– классификацию видов, методов и средств защиты информации.

уметь:

– анализировать состояние экономической безопасности организации и правильно определять роль защиты информации в ее обеспечении;

– выбирать методы определения ущерба, наносимого владельцу информации в результате противоправного ее использования;

– определять расчетным и экспертным методами стоимостные оценки ущерба, наносимого владельцу информации;

– анализировать экономическую информацию, возникающую в процессе производственно-хозяйственной деятельности, и вырабатывать рекомендации по экономической целесообразности ее защиты;

– выбирать методы сопоставительного анализа эффективности инвестиционных проектов в защиту информации;

– анализировать и классифицировать риски, возникающие при защите информации, изыскивать методы их расчетов;

– определять объекты систем защиты информации, подлежащие первоочередному страхованию, и участвовать в разработке договоров о страховании.

владеть:

– основами определения ценности информации;

– специальной профессиональной терминологией;

– основными экономическими методами защиты информации.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Теория экономики защиты информации.

Раздел 2 Защита информации в производственно-хозяйственной деятельности.

Аннотация рабочей программы производственной практики Б2.В.01(Н) «Производственная – научно-исследовательская работа»

1 Цели и задачи практики

Цели производственной практики:

– углубление полученных теоретических знаний, развитие навыков в постановке задач, их моделировании и решении;

– развитие умений анализировать результаты, оформить выводы;

– привитие навыков к самостоятельной научно-исследовательской работе в соответствии со специализацией.

Задачи производственной практики:

– как применить полученные теоретические знания для обеспечения ИБ информационных систем или объектов;

– освоить методы проведения теоретических и экспериментальных работ;

– использовать программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализировать и обрабатывать полученных в результате практики данных;

– изучить и применить требования и стандарты по оформлению научно-технической документации.

2 Требования к результатам прохождения практики

Производственная практика направлена на формирование компетенций:

Код компетенции	Содержание компетенции
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

В результате прохождения практики обучающийся должен:

знать:

– как применить полученные теоретические знания для обеспечения ИБ информационных систем или объектов;

– литературные и интернет источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;

– методы проведения теоретических и экспериментальных работ;

– правила эксплуатации оборудования, применяемого при обеспечении ИБ;

– методы анализа и обработки полученных в результате практики данных;

– информационные технологии в научных исследованиях, программные

– продукты, относящиеся к профессиональной сфере;

– требования и стандарты по оформлению научно-технической документации.

уметь:

– анализировать и обрабатывать полученных в результате практики данных;

– применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение из профессиональной области;

– оформить результаты практики в соответствии с требованиями и стандартами для научно-технической документации;

– окончательно сформулировать тему магистерской диссертации и обосновать целесообразность ее разработки.

владеть:

– по систематизации и обобщении научной информации по теме исследований;

– по теоретическому по программно-аппаратному исследованию в рамках поставленных задач;

– оценки достоверности и значимости полученных результатов;

– сравнения результатов исследования с имеющимися отечественными и зарубежными аналогами;

– использования программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализа угроз ИБ и уязвимостей в ИС;

– методами распознавания программных, сетевых, аппаратно-технических атак на объекты информатизации;

– анализ научной и практической значимости проводимых исследований.

3 Общая трудоемкость практики составляет 9 зачетных единиц или 324 часа.

4 Содержание практики

Подготовительный этап: противопожарный инструктаж и инструктаж по технике безопасности; указания по прохождению практики.

Основной этап: ознакомление с рабочим местом практики; изучение документов, литературы и других источников, необходимых для выполнения задания на практику; поиск основных Интернет-ресурсов, необходимых для выполнения задания на практику; выполнение задания на практику; анализ промежуточных результатов; получение отзыва руководителя практики от предприятия.

Заключительный этап: написание отчета по практике; защита отчета по практике; подготовка к промежуточной аттестации – зачет с оценкой.

Аннотация рабочей программы производственной практики
Б2.В.02(Н) «Производственная - научно-исследовательская работа в семестре»

1 Цели и задачи практики

Цели производственной практики:

– углубление полученных теоретических знаний применением на практике;

– развитие навыков в постановке задач, их моделировании и решении, умении анализировать результаты;

– освоение стандартов оформления результатов научно-исследовательских работ;

– привить навыки к самостоятельной научно-исследовательской работе.

Задачи производственной практики:

– освоение методов проведения теоретических и экспериментальных работ;

– освоение методов анализа и обработки полученных в результате практики данных;

– уметь оценить достоверность и значимость полученных результатов;

– знать, как распознать программные, сетевые, аппаратно-технические атаки на объекты информатизации;

– овладеть методами анализа научной и практической значимости проводимых исследований.

2 Требования к результатам прохождения практики

Производственная практика направлена на формирование компетенций:

Код компетенции	Содержание компетенции
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

В результате прохождения практики обучающийся должен:

знать:

– литературные и интернет источники по разрабатываемой теме с целью их использования при написании отчета о практике и при выполнении выпускной квалификационной работы;

– методы проведения теоретических и экспериментальных работ;

– правила эксплуатации оборудования, применяемого при обеспечении ИБ;

– методы анализа и обработки полученных в результате практики данных;

– информационные технологии в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;

– требования и стандарты по оформлению научно-технической документации.

уметь:

– анализировать и обрабатывать полученных в результате практики данных;

– применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение из профессиональной области;

– оформить результаты практики в соответствии с требованиями и стандартами для научно-технической документации;

– окончательно сформулировать тему магистерской диссертации и обосновать целесообразность ее разработки.

владеть:

– по систематизации и обобщении научной информации по теме исследований;

– по теоретическому по программно-аппаратному исследованию в рамках поставленных задач;

– оценки достоверности и значимости полученных результатов;

– сравнения результатов исследования с имеющимися отечественными и зарубежными аналогами;

– использования программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализа угроз ИБ и уязвимостей в ИС;

– анализа научной и практической значимости проводимых исследований.

3 Общая трудоемкость практики составляет 6 зачетных единиц или 216 часов.

4 Содержание практики

Подготовительный этап: оформление на практику; инструктаж по технике безопасности; инструктаж по методике выполнения задания.

Основной этап: ознакомление с рабочим местом практики; изучение документов, литературы и других источников, необходимых для выполнения задания на практику; поиск основных Интернет-ресурсов, необходимых для выполнения задания на практику; выполнение задания на практику; анализ результатов; получение отзыва руководителя практики от предприятия.

Заключительный этап: написание отчета по практике; защита отчета по практике; подготовка к промежуточной аттестации – зачет с оценкой.

Аннотация рабочей программы производственной практики Б2.В.03(П) «Производственная - по получению профессиональных умений и опыта профессиональной деятельности (предметно-ознакомительная)»

1 Цели и задачи прохождения практики

Цели производственной практики:

– углублении полученных теоретических знаний;

– Развитие навыков в постановке задач, их моделировании и решении;

– Развитие умений анализировать результаты, оформить выводы;

– Привить и развить навыки к самостоятельной научно-исследовательской работе.

Задачи производственной практики:

– как применить полученные теоретические знания для обеспечения ИБ информационных систем или объектов;

– освоить методы проведения теоретических и экспериментальных работ;

– использовать программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализировать и обрабатывать полученных в результате практики данных;

– изучить и применить требования и стандарты по оформлению научно-технической документации

2 Требования к результатам прохождения практики

Производственная практика направлена на формирование компетенций:

Код компетенции	Содержание компетенции
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

В результате прохождения практики обучающийся должен:

знать:

– как применить полученные теоретические знания для обеспечения ИБ информационных систем или объектов;

– дополнительный поиск информации и ее усвоение по преподаваемым предметам;

– литературные и интернет источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;

– методы проведения теоретических и экспериментальных работ;

– правила эксплуатации оборудования, применяемого при обеспечении ИБ;

– методы анализа и обработки полученных в результате практики данных;

– информационные технологии в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;

– требования и стандарты по оформлению научно-технической документации.

уметь:

– анализировать и обрабатывать полученные в результате практики данные;

– применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение из профессиональной области;

– оформить результаты практики в соответствии с требованиями и стандартами для научно-технической документации;

– окончательно сформулировать тему магистерской диссертации и обосновать целесообразность ее разработки.

владеть:

– по систематизации и обобщении научной информации по теме исследований;

– по теоретическому по программно-аппаратному исследованию в рамках поставленных задач;

– оценки достоверности и значимости полученных результатов;

– сравнения результатов исследования с имеющимися отечественными и зарубежными аналогами;

– использования программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализа угроз ИБ и уязвимостей в ИС;

– методами распознавания программных, сетевых, аппаратно-технических атак на объекты информатизации;

– анализ научной и практической значимости проводимых исследований.

3 Общая трудоемкость практики составляет 6 зачетных единиц или 216 часов.

4 Содержание практики

Подготовительный этап: оформление на практику; инструктаж по технике безопасности; инструктаж по методике выполнения задания.

Основной этап: ознакомление с рабочим местом практики; изучение документов, литературы и других источников, необходимых для выполнения задания на практику; поиск основных интернет-ресурсов, необходимых для выполнения задания на практику; выполнение задания на практику; анализ результатов; получение отзыва руководителя практики от предприятия.

Заключительный этап: оформление отчета по результатам практики; защита отчета научному руководителю (дифференцированный зачет).

Аннотация рабочей программы производственной практики Б2.В.04(П) «Производственная - по получению профессиональных умений и опыта профессиональной деятельности (проектная)»

1 Цели и задачи практики

Цели производственной практики:

– углубление полученных теоретических знаний, развитие навыков в постановке задач, их моделировании и решении для конкретных объектов;

– развитие практических умений планировать систему зашиты.

Задачи производственной практики:

– уметь систематизировать и обобщить научную информацию по теме исследований;

– знать, как проанализировать угрозы ИБ и уязвимостей в ИС;

– уметь сформулировать основные требования к системе защиты объекта;

– уметь составить проект системы защиты объекта;

– иметь навыки документального оформления требований к системе защиты объекта.

2 Требования к результатам прохождения практики

Производственная практика направлена на формирование компетенций:

Код компетенции	Наименование компетенции
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, 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 разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности

В результате прохождения практики обучающийся должен:

знать:

– как проанализировать применить полученные теоретические знания для обеспечения ИБ информационных систем или объектов;

– литературные и интернет источники по разрабатываемой теме с целью их использования при составлении планов по обеспечению ИБ;

– как спланировать теоретические и экспериментальные работы;

– правильно применить и эксплуатировать оборудование, применяемого при обеспечении ИБ;

– стандарты и ГОСТы по оформлению планов, проектов и технических заданий;

– информационные технологии в научных исследованиях и программные продукты;

– требования и стандарты по оформлению научно-технической документации.

уметь:

– составить план и график внедрения системы защиты конкретного объекта;

– анализировать и обрабатывать полученных в результате практики данных;

– применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение из профессиональной области;

– оформить результаты практики в соответствии с требованиями и стандартами для научно-технической документации.

владеть:

– по систематизации и обобщении научной информации по теме исследований;

– по теоретическому по программно-аппаратному исследованию в рамках поставленных задач;

– оценки достоверности и значимости полученных результатов;

– сравнения результатов исследования с имеющимися отечественными и зарубежными аналогами;

– особенности создания защищенных ИС;

– анализа угроз ИБ и уязвимостей в ИС;

– навыками планирования и проектирования систем обеспечения ИБ;

– использования программно-аппаратных средств обеспечения информационной безопасности ИС;

– анализ научной и практической значимости проводимых исследований.

3 Общая трудоемкость практики составляет 6 зачетных единиц или 216 часа.

4 Содержание практики

Подготовительный этап: противопожарный инструктаж и инструктаж по технике безопасности; указания по прохождению практики.

Основной этап: анализ предметной области (деятельности предприятия, аудит ИБ, выяснение проблем и т.п.); выявить особенности создания защищенных ИС; анализ угроз ИБ и уязвимостей в ИС; развить навыки планирования и проектирования систем обеспечения ИБ; составление плана работ и проекта системы защиты объекта; проведение исследования отдельных проблем ИБ.

Заключительный этап: оформление отчета по результатам практики; защита отчета научному руководителю (дифференцированный зачет)

Аннотация рабочей программы производственной практики Б2.В.05(П) «Производственная - по получению профессиональных умений и опыта профессиональной деятельности (организационно-управленческая)»

1 Цели и задачи практики

Цели производственной практики:

– закрепление и углубление полученных в процессе обучения теоретических знаний по ИБ;

– овладение практическими навыками и опытом управления организациями в области ИБ;

– знакомство с принятием управленческих решений в конкретных ситуациях.

Задачи производственной практики:

– знать предметную область исследования, теорию и методы управления проектами ИБ;

– знать, как оценить эффективность процесса управления ИБ предприятия.

– уметь правильно применить и эксплуатировать оборудование, применяемого при обеспечении ИБ;

– овладеть конкретными методами управления ИБ, используемыми на предприятии и/или в подразделении предприятия - базе практики;

– получить навыки анализа и организации работы предприятия в области ИБ;

– владеть навыками представления и презентации результатов исследований, аргументации и отстаивания, собственной позиции по проблемам ИБ.

2 Требования к результатам прохождения практики

Производственная практика направлена на формирование компетенций:

Код компетенции	Наименование компетенции
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

В результате прохождения практики обучающийся должен:

знать:

– как проанализировать применить полученные теоретические знания для анализа ИБ информационных систем или объектов;

– современные тенденции и перспективы научных исследований в области ИБ;

– предметной области теории и методики управления проектами ИБ;

– как оценить эффективности процесса управления ИБ предприятия.

– правильно применить и эксплуатировать оборудование, применяемого при обеспечении ИБ;

– стандарты и ГОСТы по оформлению планов, проектов и технических заданий.

уметь:

– провести сбор фактических данных о средствах, методах работы объекта практики в области организации ИБ;

– сформировать и разработать дополнительные предложения по совершенствованию процесса управления ИБ предприятия;

– систематизировать и обосновать информацию, вносимой в отчет по производственной организационно-управленческой деятельности предприятия в области ИБ.

владеть:

– конкретными методами управления ИБ, используемыми на предприятии и/или в подразделении предприятия - базе практики;

– практическими навыками анализа и организации работы предприятия в области информационной безопасности;

– навыками представления и презентации результатов исследований, аргументации и отстаивания, собственной позиции по проблемам ИБ.

3 Общая трудоемкость практики составляет 6 зачетных единиц или 216 часа.

4 Содержание практики

Подготовительный этап: противопожарный инструктаж и инструктаж по технике безопасности; указания по прохождению практики.

Основной этап: исследование организационной и управленческой структуры, особенностей предприятия; исследование функций отдельных подразделений; исследование существующих мер защиты, применяемых программных, аппаратных, физических и организационных мер защиты; анализ внешних и внутренних угроз, уязвимостей и методов противодействия; проведение оценки эффективности процесса управления ИБ.

Заключительный этап: оформление отчета по результатам практики; защита отчета научному руководителю (дифференцированный зачет).

Аннотация рабочей программы производственной практики Б2.В.06(Пд) «Производственная - преддипломная»

1 Цели прохождения практики

Цели производственной практики:

– закрепление полученных в вузе теоретических и практических знаний; подбор материалов, проведение испытания и тестирования систем и технологий информационной безопасности, разработанных в соответствии с заданием на выпускную квалификационную работу; закрепление профессиональных умений и навыков управления информационной безопасностью предприятия;

– адаптация к рынку труда по конкретному направлению подготовки;

– приобретение учащимся опыта в исследовании актуальной научной проблемы или решении реальной задачи по информационной безопасности.

Задачи производственной практики:

– закрепление и углубление теоретической подготовки обучающегося;

– сбор материалов в соответствии с заданием на выпускную квалификационную работу;

– оценка научной новизны и практической значимости;

– оформление, полученных результатов (предварительной рукописи ВКР).

2 Требования к результатам прохождения практики

Прохождение производственной практики направлено на формирование компетенций:

Код компетенции	Наименование компетенции
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения
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-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-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

В результате прохождения практики обучающийся должен:

знать:

– предметную область проводимого квалификационного исследования;

– тему выпускной квалификационной работы в окончательном виде по профилю направления «Безопасность информационных систем и технологий»;

уметь:

– применять базовые методики исследования, выполнять сравнительный анализ полученных результатов;

– обосновать целесообразность разработки темы;

– подобрать необходимые источники по теме (литературу, патентные материалы, научные отчеты, техническую документацию и др.) и провести их анализ;

владеть:

– необходимыми знаниями, алгоритмами, моделями и др. для выполнения предусмотренного планом объем исследований по реализации темы;

– методами обработки имеющихся данных и анализа достоверности полученных результатов для подготовки собранного материала к оформлению магистерской диссертации;

– методиками научного поиска и анализа.

3 Общая трудоемкость практики составляет 18 зачетных единицы, 648 часов.

4 Содержание практики

Подготовительный этап: оформление на практику; инструктаж по технике безопасности; инструктаж по методике выполнения задания.

Основной этап: ознакомление с рабочим местом практики; изучение проектно-технической документации; разработка технического задания; выполнение задания на преддипломную практику; обработка и анализ полученных результатов.

Заключительный этап: оформление документов и защита отчета научному руководителю (дифференцированный зачет).

Аннотация рабочей программы дисциплины
Б3.Б.01 «Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты»

1 Цели и задачи освоения дисциплины «Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты».

Цель освоения дисциплины:

– проверка теоретических знаний, практических умений и навыков обучающегося, а также способности их применения во всех областях профессиональной деятельности с учетом специфики и содержательного наполнения образовательной программы;

– оценка конечного результата проделанной обучающимся научно-исследовательской и практической работы, свидетельствующей о полученной квалификации, о приобретенном опыте работы, об умении решать сложные задачи, свободно ориентироваться в научной и технической литературе, об умении грамотно излагать свои мысли, а также передавать свои знания коллегам по профессиональной деятельности;

– проверка качества сформированности общекультурных, общепрофессиональных и профессиональных компетенций по направлению подготовки 10.04.01 Информационная безопасность;

Задачи освоения дисциплины:

– определение уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям ФГОС ВО и профессионального стандарта.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
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
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, 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 разрабатывать 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	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи
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

Выпускная квалификационная работа обучающегося имеет целью показать:

– уровень профессиональной и общеобразовательной подготовки выпускника по направлению подготовки 10.04.01 Информационная безопасность профиль «Безопасность информационных систем и технологий»;

– умение изучать и обобщать литературные источники в области информационной безопасности;

– способность самостоятельно проводить научные исследования теоретического и прикладного характера, выполнять аналитические работы, систематизировать и обобщать фактический материал;

– умение самостоятельно обосновывать выводы и практические рекомендации по результатам проведенных исследований (работы).

3 Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

4 Содержание дисциплины

Раздел 1 Изучение литературы по проблеме, определение целей, задач и методов исследования.

Раздел 2 Непосредственная разработка проблемы (темы): теоретические и прикладные исследования.

Раздел 3 Обобщение и оценка полученных результатов исследования (работы).

Раздел 4 Написание и оформление ВКР.

Раздел 5 Рецензирование работы.

Раздел 6. Подготовку к защите ВКР.

Раздел 7. Защита и оценка работы.

Аннотация рабочей программы дисциплины
ФТД.В.01 «Основы научных исследований»

1 Цели и задачи освоения дисциплины «Основы научных исследований».

Цель освоения дисциплины:

– формирование у обучающихся знаний, умений и навыков для выполнения самостоятельных научных исследований в области информационной безопасности

Задачи освоения дисциплины:

– обучить анализу литературы и проведения патентного поиска с целью определения направления исследований;

– обучить разработке программы теоретических и экспериментальных исследований, ее реализация, включая выбор технических средств и обработку результатов;

– обучить построению математических моделей объектов и процессов; выбор метода их исследования и разработка алгоритма его реализации;

– обучить моделированию объектов и процессов с целью анализа и оптимизации их параметров;

– обучить анализу возможностей получения патентов на полезные модели и\или на изобретения;

– научить составлять обзоры и отчеты по результатам проводимых исследований.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Основы научных исследований» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ОК-1	способность к абстрактному мышлению, анализу, синтезу
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам

В результате освоения дисциплины обучающийся должен:

знать:

– как анализировать литературы и проводить патентный поиск с целью определения направления исследований;

– как разрабатывать программы теоретических и экспериментальных исследований, как их реализовать, включая выбор технических средств и обработку результатов;

– как строить математические модели объектов и процессов; выбирать методы их исследования и разрабатывать их алгоритмы реализации;

– моделирование объектов и процессов с целью анализа и оптимизации их параметров;

– анализ возможностей получения патентов на полезные модели и\или на изобретения;

– составление обзоров и отчетов по результатам проводимых исследований.

уметь:

– проводить анализ литературы и проведение патентного поиска с целью определения направления исследований;

– разрабатывать программы теоретических и экспериментальных исследований, ее реализация, включая выбор технических средств и обработку результатов;

– строить математические модели объектов и процессов; выбирать методы их исследования и разрабатывать алгоритмы их реализации;

– моделировать объекты и процессы с целью анализа и оптимизации их параметров;

– анализ возможностей получения патентов на полезные модели и\или на изобретения;

– составление обзоров и отчетов по результатам проводимых исследований.

владеть:

– навыками анализа литературы и проведения патентного поиска с целью определения направления исследований;

– навыками разработки программы теоретических и экспериментальных исследований, ее реализация, включая выбор технических средств и обработку результатов;

– навыками построения математических моделей объектов и процессов; выбор метода их исследования и разработка алгоритма его реализации;

– навыками моделирования объектов и процессов с целью анализа и оптимизации их параметров.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Введение. Основные этапы развития науки.

Раздел 2 Основные определения и понятия в системе научных знаний.

Раздел 3 Организация научно-исследовательской работы в Российской Федерации.

Раздел 4 Научные исследования. Основные этапы и использование результатов.

Раздел 5 Методология научного исследования.

Раздел 6 Особенности экспериментального исследования.

Раздел 7 Теоретические исследования.

Раздел 8 Виды СРС.

Раздел 9 Научные документы и издания.

Аннотация рабочей программы дисциплины
ФТД.В.02 «Информационно - аналитические системы безопасности»

1 Цели и задачи освоения дисциплины «Информационно - аналитические системы безопасности».

Цель освоения дисциплины:

– формирование представления об информационно-аналитических системах безопасности, типовой структуре КИС, методиках анализа и активного аудита безопасности такого класса систем, а также о наиболее вероятных угрозах ИБ в КИС

Задачи освоения дисциплины:

– получение обучающимся знаний:

– об информационно-аналитической поддержке принятия решений на основе мониторинга и ситуационного анализа;

– о применение автоматизированных технологий информационно-аналитической деятельности;

– о применение моделей, методов и алгоритмов решения типовых задач обработки и анализа информации в автоматизированных информационно-аналитических системах, обеспечивающих обработку и анализ специальной информации (в дальнейшем - специальных АИС);

– о применение автоматизированных средств обеспечения информационно-аналитической деятельности;

– об информационно-аналитическом обеспечение предупреждения, пресечения, выявления, раскрытия и расследования правонарушений;

– об обеспечение информационно-аналитической составляющей процессов мониторинга в социально-экономической, финансовой и правоохранительной сферах.

2 Требования к результатам освоения дисциплины

Освоение дисциплины «Информационно - аналитические системы безопасности» направлено на формирование компетенций:

Код компетенции	Содержание компетенции
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств

ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам
ПК-13	способность организовать управление информационной безопасностью

В результате освоения дисциплины обучающийся должен:

знать:

– базовые способы оценки и повышения защищенности информационных ресурсов в корпоративной информационной системы (КИС);

– способы инвентаризации программных сервисов и информационных ресурсов;

– ключевые точки приложения информационных атак в типовой структуре КИС;

– активные и пассивные методы сбора информации;

– информационные источники и аналитические методы конкурентной разведки;

– систему мер противодействия промышленному шпионажу;

– технологии в системе информационно-аналитического обеспечения безопасности;

уметь:

– осуществлять выбор функциональной структуры системы обеспечения информационной безопасности (ИБ);

– проводить мониторинг и выявление условий, способствующих совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных и других сведений ограниченного распространения;

– ставить и решать типовые задачи в области оценки и повышения защищенности КИС, подбирать и использовать адекватные методы и средства защиты информации, оценивать эффективность методов защиты информационных процессов;

владеть:

– навыками аудита ИБ с использованием современных программно-технических средств;

– приемами тестирования уязвимостей корпоративных программно-технических сервисов, современным аппаратом для количественной и качественной оценки результатов аудита,

– навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений;

– способами разработки технического задания и проектных документов на разработку специальных АИС и средства обеспечения их безопасности.

3 Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

4 Содержание дисциплины

Раздел 1 Основные уязвимости КИС.

Раздел 2 Информационно-аналитическая деятельность в системе безопасности.

Раздел 3 Требования к информационно-аналитической системе службы безопасности.

Раздел 4 Основные способы проведения инвентаризации программно-технических средств и сетевых служб. Средства негласной инвентаризации.

Раздел 5 Конкурентная разведка; технологии сбора следовой информации; методы компьютерной разведки.

Раздел 6 Противодействие промышленному шпионажу.

Раздел 7 Информационные технологии в системе информационно-аналитического обеспечения безопасности.