

Приложение 3. Аннотации рабочих программ дисциплин,
практик и государственной итоговой аттестации

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНЫ
приказом и.о. ректора
от «17» июня 2022 г. № 76

**АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН,
ПРАКТИК И ГОСУДАРСТВЕННОЙ ИТОГОВОЙ
АТТЕСТАЦИИ**

**ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ
ПРОГРАММЫ ВЫСШЕГО ОБРАЗОВАНИЯ**

НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.04.01 Информационная безопасность

ПРОФИЛЬ ПОДГОТОВКИ
Безопасность информационных систем и технологий

Квалификация выпускника – Магистр
Форма и срок обучения – очная форма 2 года
Год начала подготовки – 2022 год
Общая трудоемкость – 120 з.е.
Выпускающая кафедра – Информационные системы и защита информации

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.

00a73c5b7b623a969ccad43a81ab346d50 с 08.12.2022 14:32 по 02.03.2024 14:32 GMT+03:00

Подпись соответствует файлу документа



Аннотация рабочей программы дисциплины Б1.О.01 Критическое мышление

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- выработка у обучающихся рационального, проблемно-ориентированного, критического мышления;
- формирование общеметодологических оснований познавательной и профессиональной деятельности.

Задачи дисциплины:

- овладение навыками логически правильного и познавательно продуктивного мышления;
- умение воспринимать и оценивать получаемую информацию с точки зрения ее точности и достоверности, строить логически корректную и убедительную собственную аргументацию;
- способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических проблем.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	УК-1.1 Анализирует проблемную ситуацию, определяет причины ее возникновения и осуществляет её декомпозицию на отдельные задачи	Знать: законы и принципы правильного мышления; методы критического анализа проблемных ситуаций
		Уметь: анализировать информацию с позиции ее логической правильности и обоснованности; определять причины возникновения проблемных ситуаций
		Владеть: навыками анализа проблемной ситуации и причин ее возникновения; приемами логического анализа высказываний и построения доказательного рассуждения
	УК-1.2 Вырабатывает стратегию достижения поставленной цели	Знать: принципы и методы выработки стратегии достижения поставленной цели; основные методы принятия решений
		Уметь: формулировать гипотезы, цели и пути достижения теоретических и практических целей; выработать стратегию действий и логику принятия решений
		Владеть: навыками логически правильного и познавательно продуктивного мышления для достижения поставленной цели; применять методы и приемы критического мышления в профессиональной теоретической и практической деятельности

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

4 Содержание дисциплины

Раздел 1. Критическое мышление: основные проблемы и понятия

Раздел 2. Логические основы мышления

Раздел 3. Принятие решений

**Аннотация рабочей программы дисциплины
Б1.О.02 Основы научных исследований**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- формирование у студентов знаний, умений и навыков для выполнения самостоятельных научных исследований в области информационной безопасности.

Задачи дисциплины:

- разработка программы теоретических и экспериментальных исследований, ее реализация, включая выбор технических средств и обработку результатов;
- построение математических моделей объектов и процессов; выбор метода их исследования и разработка алгоритма его реализации;
- моделирование объектов и процессов с целью анализа и оптимизации их параметров;
- составление обзоров и отчетов по результатам проводимых исследований.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию, определяет причины ее возникновения и осуществляет её декомпозицию на отдельные задачи	Знать: как анализировать проблемную ситуацию, определять причины ее возникновения; как осуществлять декомпозицию проблемной ситуации на отдельные задачи
		Уметь: анализировать проблемную ситуацию, определять причины ее возникновения; осуществлять декомпозицию проблемной ситуации на отдельные задачи
		Владеть: методами анализа проблемных ситуаций, определения причин их возникновения; подходами к осуществлению декомпозиции проблемной ситуации на отдельные задачи
	УК-1.2 Вырабатывает стратегию достижения поставленной цели	Знать: как вырабатывать стратегию достижения поставленной цели
Уметь: вырабатывать стратегию достижения поставленной цели		
Владеть: навыками формирования стратегии достижения поставленной цели		
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.3 Использует информационно-коммуникационные технологии для поиска, обработки и представления информации	Знать: как анализировать научную литературу и проводить патентный поиск с целью определения направления исследований; как составлять обзоры и отчеты по результатам проводимых исследований
		Уметь: анализировать научную литературу и проводить патентный поиск с целью определения направления исследований; использовать информационно-коммуникационные технологии для поиска и подготовки научных исследований
		Владеть: навыками анализа научной литературы и проведения патентного

		поиска с целью определения направления исследований; навыками использования информационно-коммуникационные технологии для поиска информации
	УК-4.4 Представляет результаты академической и профессиональной деятельности на публичных мероприятиях	Знать: как представлять результаты академической и профессиональной деятельности на публичных мероприятиях
		Уметь: представлять результаты академической и профессиональной деятельности на публичных мероприятиях
		Владеть: навыками представления результатов академической и профессиональной деятельности на публичных мероприятиях

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

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.

Аннотация рабочей программы дисциплины Б1.О.03 Лидерство и командообразование

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- формирование у обучающихся теоретических знаний о лидерстве и командообразовании, создание условий для развития управленческих компетенций и личностного роста.

Задачи дисциплины:

- сформировать у обучающихся знания в области командной работы и развития лидерских качеств;

- сформировать у обучающихся умения в области выбора подходов и методов к осуществлению командной работы и развития лидерских качеств;

- сформировать у обучающихся навыки командной работы и проявления лидерских качеств.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-3. Способен организовывать и руководить работой команды, выработывая командную стратегию для достижения поставленной цели	УК-3.1 Демонстрирует понимание принципов командной работы	Знать: основы командообразования; основные теории лидерства; жизненный цикл команды; условия результативности команды
		Уметь: проявлять лидерские качества; выявлять стадию командообразования
	УК-3.2 Ставит задачи перед членами команды, руководит ими для достижения поставленной задачи	Знать: жизненный цикл команды; условия результативности команды
		Уметь: анализировать состав команды Владеть: навыками формирования стратегии для достижения цели
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания	Знать: основы проведения самооценки; методы, способы и инструменты оценки своих ресурсов
		Уметь: оценивать свои ресурсы, в том числе лидерские; оптимально использовать свои ресурсы для выполнения порученных заданий; планировать процесс развития своих ресурсов
		Владеть: способами совершенствования собственной деятельности на основе самооценки; навыками обоснования применяемых методов, способов и инструментов развития своих ресурсов; навыками определения эффективности применяемых методов, способов и инструментов развития своих ресурсов

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

4 Содержание дисциплины

Раздел 1. Лидерство.

Раздел 2. Командообразование.

**Аннотация рабочей программы дисциплины
Б1.О.04 Иностранный язык в профессиональной деятельности**

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования;
- формирование у обучающихся способности и готовности к коммуникации на иностранном языке в рамках профессиональной и научной деятельности.

Задачи дисциплины:

- совершенствование навыков и умений монологического и диалогического высказывания;
- совершенствование навыков изучающего, просмотрового и поискового чтения, а также перевода текстов, представляющих личностный, профессиональный и научный интерес;
- совершенствование навыков представления проектного материала по профессиональной и научной тематике (доклады, мультимедийные презентации, сообщения, пр.);
- повышение уровня учебной автономии, способности к самообразованию;
- развитие когнитивных и исследовательских умений;
- развитие информационной культуры.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 Способен к устной и письменной коммуникации по профессионально релевантным темам на иностранном языке	Знать: основные особенности делового и профессионального дискурса; базовую лексику, представляющую деловой профессиональный стиль, а также основную терминологию своей специальности; лексико-грамматические конструкции в описании графиков, таблиц, схем
		Уметь: воспринимать на слух и понимать основное содержание аутентичных публицистических (медийных) и прагматических аудиотекстов, относящихся к сфере профессиональной деятельности; понимать содержание публицистических текстов, блогов/веб-сайтов по профессиональной тематике; продуцировать монологические и диалогические высказывания на профессиональные темы, высказывать свое мнение о прочитанном (услышанном), делать сообщения, выстраивать монолог-описание на основе нелинейных текстов (графики, схемы, таблицы); продуцировать письменные высказывания профессионального характера в соответствии с коммуникативной задачей и принятым форматом; вести запись основных мыслей и фактов (из аудиотекстов и текстов для чтения)
		Владеть: навыками устного и письменного выражения собственной точки зрения с элементами аргументации; навыками публичного представления и обсуждения

		результатов исследования по профессиональным темам
	УК-4.2 Способен к извлечению информации из отечественных и зарубежных источников научного характера с последующей переработкой (компрессией) в виде обзора, аннотации, реферата, доклада, презентации на иностранном языке	Знать: отличительные особенности отечественного и зарубежного (изучаемого языка) научного дискурса; базовую лексику, представляющую нейтральный научный стиль, а также основную терминологию своей научной специальности, лексико-грамматические конструкции, характерные для этапов реферирования и аннотирования научных и медийных текстов; основные принципы и приемы перевода технического текста
		Уметь: воспринимать на слух и понимать основное содержание аутентичных публицистических (медийных) и прагматических аудиотекстов, относящихся к сфере научной деятельности; понимать содержание научно-популярных и научных текстов по профессиональной тематике; выделять значимую/запрашиваемую информацию из прагматических текстов справочно-информационного характера; использовать толковые и двуязычные словари и другую справочную литературу для решения переводческих задач; вести запись тезисов устного выступления/письменного доклада по изучаемой проблематике; выполнять письменные проектные задания (оформление презентаций, докладов, рефератов статей и аннотаций)
		Владеть: иностранным языком в объеме, необходимом для получения информации из зарубежных источников; навыками поискового, ознакомительного и изучающего чтения научной и научно-популярной литературы; основными приемами реферирования и аннотирования, навыками презентации сообщения на иностранном языке

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

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.О.05 Межкультурная коммуникация

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- сформировать представление о культурных различиях, принципах культурного релятивизма, концептуальных подходах в теории межкультурной коммуникации в современном поликультурном пространстве;
- научить ориентироваться в современных научных представлениях о сущности и роли межкультурных коммуникаций, сформировать навыки эффективного социального взаимодействия с представителями различных культур.

Задачи дисциплины:

- сформировать знания об основных этапах развития межкультурной коммуникации, значимых ученых, внесших вклад в развитие межкультурной коммуникации;
- понимать и объяснять основные парадигмы в исследовании феноменов культуры и коммуникации;
- знать существующие стереотипы восприятия различных культур и способы их преодоления;
- уметь применять уметь применять методы и средства познания, обучения и самоконтроля в определенных культурно-исторических реалиях.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Демонстрирует понимание особенностей различных культур	Знать: особенности и отличия различных типов культур, их основные характеристики, культурные факторы, влияющие на социальное взаимодействие
		Уметь: применять знания о разнообразии культур в процессе межкультурного взаимодействия
		Владеть: навыками уважительного и бережного отношения к особенностям различных культур, способами преодоления культурных стереотипов
	УК-5.2 Выстраивает социальное взаимодействие, учитывая общее и особенное различных культур	Знать: важнейшие ценности различных культур, определяющие коммуникативное поведение их носителей
		Уметь: ориентироваться в проблемах межкультурной коммуникации, интерпретировать конкретные проявления коммуникативного поведения представителей различных культур
		Владеть: навыками межкультурной коммуникации, обеспечивающими продуктивное социальное взаимодействие

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

4 Содержание дисциплины

Раздел 1. Теоретические основы изучения межкультурной коммуникации.

Раздел 2. Типология культур.

Раздел 3. Межкультурная компетентность как условие эффективного межкультурного взаимодействия.

**Аннотация рабочей программы дисциплины
Б1.О.06 Моделирование технических объектов и систем управления**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

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

Задача дисциплины:

- овладение методами математического моделирования объектов технического характера и систем управления ими.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты	Знать: основные понятия применяемого математического аппарата; основные методы построения математических моделей; методы расчета и исследования математических моделей с использованием вычислительной техники
		Уметь: учитывать весь комплекс особенностей объектов исследования; разрабатывать математические модели; оценивать адекватность примененных методов моделирования
		Владеть: приемами построения математических моделей; методами исследования моделей; средствами построения прогнозов по математическим моделям
	ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ	Знать: основные понятия информационной безопасности по аттестации объектов информатизации; законодательные требования по аттестации объектов информатизации; отчетные документы по результатам проведения предпроектного обследования объектов информатизации
		Уметь: применять понятия информационной безопасности по аттестации объектов информатизации; оперировать законодательные требования по аттестации объектов информатизации; составлять отчетные документы по результатам проведения предпроектного обследования объектов информатизации
		Владеть: понятийным аппаратом информационной безопасности по аттестации объектов информатизации; навыками работы с законодательными документами по аттестации объектов информатизации; навыками составления отчетных документов по результатам проведения предпроектного обследования объектов информатизации

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

4 Содержание дисциплины

- Раздел 1. Понятие «модель». 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.О.07 Информационная безопасность критической информационной
инфраструктуры

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- формирование у студентов системных знаний по обеспечению информационной безопасности критической информационной инфраструктуры, а также практических навыков по разработке и реализации планов реагирования на компьютерные инциденты.

Задачи дисциплины:

- формирование системных знаний о значимых объектах критической информационной инфраструктуры, а также методах и средствах обеспечения их безопасности;

- изучение нормативно-правовых актов по безопасности критической информационной инфраструктуры;

- изучение методов оценки уровня защищенности (аудита) систем и сетей и содержащейся в них информации;

- освоение необходимых знаний по проведению категорирования объектов критической информационной инфраструктуры;

- формирование умений и знаний по проведению оценки угроз безопасности информации на объектах критической информационной инфраструктуры;

- изучения механизма проведения инвентаризации систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;

- освоение методов организации и планирования мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает основные виды организационно-распорядительных документов в области ИБ, требования по формированию политик ИБ, защите компьютерных систем и сетей	Знать: нормативно правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ; основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования
		Уметь: определить категорию значимости объектов КИИ; выявлять и анализировать угрозы безопасности информации по результатам возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации; обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ
		Владеть: навыками работы с нормативно правовыми актами, методическими документами и национальными стандартами в области обеспечения безопасности значимых

		<p>объектов КИИ; навыками работы с базами данных, содержащую информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами; навыками эксплуатации системы безопасности значимого объекта КИИ</p>
	<p>ОПК-3.2 Умеет разрабатывать организационно-распорядительные документы и формировать политику в области информационной безопасности</p>	<p>Знать: основные принципы выявления наличия критических процессов у субъекта КИИ; основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль и мониторинг критических процессов; процедуры выявления и анализ угроз безопасности информации, обрабатываемой объектом КИИ; общие требования по обеспечению безопасности значимых объектов КИИ; цели, задачи, основные принципы организации государственного контроля области обеспечения безопасности значимых объектов КИИ</p> <p>Уметь: определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ; определять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и аппаратными средствами, функцией безопасности этих средств и особенностями их реализации, а также категории значимого объекта КИИ</p> <p>Владеть: навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ; навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ</p>

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

4 Содержание дисциплины

Раздел 1. Основы обеспечения безопасности значимых объектов КИИ.

Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ.

Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ.

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

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- 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;

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

Задача дисциплины:

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

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1 Знает требования к оформлению технического проекта системы обеспечения ИБ и особенности его разработки	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; 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; 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
	ОПК-2.2 Умеет разрабатывать технический проект системы ИБ,	Знать: принципы и методы обработки конфиденциальных документов в потоках при любых используемых типах систем и способах

	выбирать технологии защиты обеспечивающей части информационно-аналитической системы (ИАС)	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; требования к оформлению технического проекта системы обеспечения ИБ; особенности разработки технического проекта системы
		Уметь: формулировать задачи по разработке потребительских требований к автоматизированным системам обработки и хранения конфиденциальных документов; разрабатывать и совершенствовать немашинную часть организации и технологии функционирования автоматизированных систем обработки и хранения конфиденциальных документов; разрабатывать технический проект системы ИБ; выбирать технологии защиты обеспечивающей части информационно-аналитической системы (ИАС)
		Владеть: основными элементами защиты и обработки конфиденциальных документов; технологиями защиты информационно-аналитических систем

3 Общая трудоемкость дисциплины составляет 180 часов, 5 зачетных единиц.

4 Содержание дисциплины

Раздел 1. Бумажный конфиденциальный документооборот.

Раздел 2. Электронный конфиденциальный документооборот.

**Аннотация рабочей программы дисциплины
Б1.О.09 Теория систем и системный анализ**

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- формирование целостного представления у магистрантов о месте и роли теории систем и системного анализа в процессе исследования и разработки современных сложных систем, моделирующих проблемную ситуацию в области информационной безопасности;
- изучение основных положений и понятий системного анализа.

Задачи дисциплины:

- овладение навыками применения методов системного анализа при описании и разложении сложных объектов на простые методом декомпозиции;
- умение осуществлять сбор, обработку, анализ и систематизацию научных результатов при исследовании сложных объектов.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты	Знать: порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты; как обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
		Уметь: проводить предпроектное обследование объектов информатизации, средства и особенности их защиты; обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
		Владеть: навыками проведения предпроектного обследования объектов информатизации, средства и особенности их защиты; навыками обоснования требования к системе обеспечения информационной безопасности и разработки проекта технического задания на ее создание
	ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ	Знать: как оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ
		Уметь: оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ
		Владеть: навыками оформления результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ

3 Общая трудоемкость дисциплины составляет 144 часа, 4 зачетные единицы.

4 Содержание дисциплины

- Раздел 1. Принципы системного анализа, состояния и функционирование систем.
- Раздел 2. Структуры и классификация систем, этапы системного анализа.
- Раздел 3. Модели и моделирование, уровни и методы моделирования.
- Раздел 4. Методы исследования операций в системном анализе.
- Раздел 5. Кибернетические системы, типы и методы исследования.

Аннотация рабочей программы дисциплины Б1.О.10 Специальные разделы математики

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- овладение студентами специальным математическим инструментарием, необходимым для решения профессиональных задач в сфере информационной безопасности, проведения научных исследований, обработки результатов научных исследований.

Задачи дисциплины:

- формирование умения решать прикладные задачи с использованием современных информационных технологий, готовить доклады и отчеты по выполненной работе;
- усвоение обучающимися порядка и особенностей исследований в области информационной безопасности, требований к оформлению научной и деловой документации.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1 Знает порядок проведения и особенности исследований в области информационной безопасности, требования к оформлению научной и деловой документации	Знать: основные типы статистических задач и математические методы их решения; основные теоретико-числовые методы применительно к задачам защиты информации
		Уметь: проводить экспериментальные исследования; обрабатывать результаты исследований
		Владеть: навыками аналитического и численного решения задач математической статистики; навыками расчета и оценки криптографических систем
	ОПК-5.2 Умеет решать прикладные задачи с использованием современных информационных технологий, готовить доклады и отчеты по выполненной работе	Знать: порядок и особенности исследований в области информационной безопасности; требования к оформлению научной и деловой документации
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 исследования и моделирования сложных систем и процессов, навыками проверки полученных моделей на адекватность; навыками презентации и интерпретации полученных результатов		

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

4 Содержание дисциплины

Раздел 1. Теория случайных процессов.

Раздел 2. Математические основы защиты информации.

Аннотация рабочей программы дисциплины Б1.О.11 Экономика и управление

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- формирование у обучающихся понимания закономерностей и процессов, проходящих в экономических системах на микро- и макроуровне, способности использовать экономические знания в различных сферах жизнедеятельности;
- формирование у обучающихся профессиональных компетенций, необходимых для принятия управленческих решений при работе на производственных предприятиях и в организациях различных организационно-правовых форм и различных отраслей народного хозяйства.

Задачи дисциплины:

- сформировать у обучающихся систему современных экономических знаний в области экономики организации (предприятия) и принципами ее эффективного функционирования, в том числе на предприятиях железнодорожного транспорта;
- рассмотреть основные функции, место и роль организации (предприятия) в современной экономике;
- сформировать у обучающихся умения анализировать экономические процессы и явления и использовать полученные результаты в своей профессиональной деятельности. - изучить основные принципы и направления эффективного использования ресурсов организации (предприятия);
- сформировать практические навыки по оценке эффективности функционирования и анализу деятельности организации (предприятия);
- научить современным методам расчета, планирования и анализа технико-экономических показателей деятельности организации (предприятия).

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	Знать: основные тенденции развития организации (предприятия), в том числе транспортного комплекса, как основного звена всей экономики в условиях обеспечения ИБ; понятия основные и оборотные средства и методы оценки эффективности их использования; понятие себестоимости и методы калькуляции затрат на обеспечение информационной безопасности на предприятиях (организациях); формы и методы оплаты труда; методы оценки экономической эффективности реализации проектов в области ИБ;
		Уметь: применять методы управления материальными и трудовыми ресурсами, в том числе на предприятиях железнодорожного транспорта; проводить экономическую оценку эффективности реализации проектов в области ИБ;
		Владеть: методами планирования и анализа эффективности использования материальных и трудовых ресурсов на предприятии; методами калькулирования затрат на обеспечение ИБ; навыками оценки

		экономической эффективности технических разработок и программ в области ИБ
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач	Знать: способы и методы сбора и анализа исходных данных; базовые инструментальные средства необходимые для обработки данных и их понятия; основные информационные технологии обработки данных в соответствии с поставленной задачей
		Уметь: осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности; использовать эти знания в при решении поставленных задач
		Владеть: способностью осуществлять сбор, анализ и обработку данных для решения профессиональных задач; основами сбора и анализа необходимой информации для решения поставленных задач

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

4 Содержание дисциплины

Раздел 1. Предприятие в системе информационной безопасности.

Раздел 2. Экономические ресурсы предприятия.

Раздел 3. Финансовые результаты и оценка экономической эффективности проектов информационной безопасности.

**Аннотация рабочей программы дисциплины
Б1.О.12 Защищенные информационные системы**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- формирование у студентов системных знаний по созданию и эксплуатации защищенных информационных систем, безопасных продуктов и систем информационных технологий, а также методов противодействия угрозам безопасности.

Задачи дисциплины:

- изучение методов оценки уровня защищенности информационных систем;
- освоение необходимых знаний по изучению методам противодействия угрозам безопасности;
- формирование умений и знаний по созданию и эксплуатации защищенных информационных систем;
- освоение методов организации и планирования мероприятий по обеспечению безопасности информационных систем;
- изучение методов оценки уровня защищенности информационных систем;
- освоение необходимых знаний по изучению методам противодействия угрозам безопасности;
- формирование умений и знаний по созданию и эксплуатации защищенных информационных систем.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия	Знать: методы управления проектами; этапы жизненного цикла проекта; модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления, оформления и утверждения
		Уметь: анализировать структуру, порядок составления, оформления и утверждения Технического задания по созданию АС, и изделий ИС, а также состав и структуру основных документов
		Владеть: навыками выбора наиболее эффективных методов управления проектами на этапах их жизненного цикла
	УК-2.2 Осуществляет эффективное управление проектом на всех этапах жизненного цикла для достижения конечного результата	Знать: состав и структуру основных документов; 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
		Уметь: анализировать: методы управления проектами; этапы жизненного цикла при. создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС
		Владеть: навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты

		информации в ИС и внедрения их в практику на всех этапах жизненного цикла
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.2 Определяет приоритеты личностного роста и способы совершенствования собственной деятельности на основе самооценки и самообучения	Знать: свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания, а также возможности их самостоятельного, критического изучения и осмысления
		Уметь: определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям
		Владеть: способностью выстраивать гибкую профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты	Знать: порядок и требования к проведению предпроектного обследования объектов информатизации; понятие, виды и структуру автоматизированных систем; понятие и составляющие безопасности автоматизированных систем; схемы каталогизации угроз безопасности КС, способы их идентификации, спецификации и оценивая, роль человеческого фактора в угрозах безопасности ИС; понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности ИС
		Уметь: идентифицировать и оценивать угрозы безопасности при проведении предпроектного обследования ИС; определять и оформлять класс защищенности, проектируемой ИС
	Владеть: навыками работы с требованиями нормативно-правовых актов и нормативно-методических документов в сфере защиты информации при проведении предпроектного обследования объектов информатизации	
	ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ	Знать: общую характеристику и методологию руководящих документов ФСТЭК по защите средств вычислительной техники (СВД) и автоматизированных систем (АС) от несанкционированного доступа к информации, классы защищенности и структуру функциональных требований к подсистемам защиты информации; общую характеристику и структуру стандартов по безопасности информационных технологий
		Уметь: составлять и правильно оформлять основные разделы Технического задания на проектирование несложных ИС (системы защиты информации ИС)
	Владеть: навыками проведения предпроектного обследования ИС на предмет проектирования систем защиты информации	

3 Общая трудоемкость дисциплины составляет 288 часов, 8 зачетных единиц.

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 безопасности ИС.

Аннотация рабочей программы дисциплины

Б1.О.13 Управление информационной безопасностью автоматизированных систем

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

– применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачи дисциплины:

– приобретение необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;

– формирование у обучаемых целостного представления об организации и сущности процессов управления информационной безопасностью (ИБ) на предприятии как результата внедрения системного подхода по решению задач обеспечения ИБ.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	Знать: основные направления и тенденции развития технологий в области ИБ
		Уметь: разрабатывать планы и программы по основным направлениям и тенденциям развития технологий в области ИБ
		Владеть: навыками по основным направлениям и тенденциям развития технологий в области ИБ
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач	Знать: методы сбора, обработки и анализа научно-технической информации
		Уметь: разрабатывать планы и программы проведения научных исследований и технических разработок
		Владеть: навыками работ по сбору, обработке и анализу научно-технической информации по теме исследования

3 Общая трудоемкость дисциплины составляет 180 часов, 5 зачетных единиц.

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.О.14 Экспертные системы информационной безопасности**

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- формирование представления о технологии экспертных систем (ЭС) и основных задачах информационной безопасности (ИБ), решаемых средствами ЭС;
- получение знаний в области применения технологии ЭС для решения проблем информационной безопасности (ИБ).

Задачи дисциплины:

- ознакомить с современными технологиями моделирования знаний и рассуждений;
- теоретическое и практическое освоение методов разработки ЭС для решения задач информационной безопасности.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1 Знает порядок проведения и особенности исследований в области информационной безопасности, требования к оформлению научной и деловой документации	Знать: основы технологии ЭС, базовые положения теории ЭС и знаниевого моделирования; порядок оформления докладов и отчетов по темам дисциплины
		Уметь: применить базовые положения теории ЭС к задачам ИБ; представлять результаты в виде отчетов и докладов
		Владеть: навыками составления отчетной документации по выполненным работам; навыками публичного выступления по направлению ЭС в ИБ
	ОПК-5.2 Умеет решать прикладные задачи с использованием современных информационных технологий, готовить доклады и отчеты по выполненной работе	Знать: классические и неклассические модели знаний и рассуждений; инструментальные и языковые средства разработки ЭС
Уметь: решать задачи ИБ на основе технологий ЭС с использованием языковых и инструментальных средств		
Владеть: навыками работы с инструментальными и языковыми средствами ЭС		

3 Общая трудоемкость дисциплины составляет 216 часов, 6 зачетных единиц.

4 Содержание дисциплины

Раздел 1 Введение в экспертные системы (ЭС).

Раздел 2 Моделирование знаний.

Раздел 3 Моделирование рассуждений.

Раздел 4 Разработка и эксплуатация ЭС

**Аннотация рабочей программы дисциплины
Б1.В.ДВ.01.01 Проектирование информационных систем**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- получение углубленных знаний и формирование компетенций в области методологических и прикладных вопросов проектирования информационных систем в области информационной безопасности.

Задачи дисциплины:

- особенности поддержки жизненного цикла информационных систем;
- использование методологий проектирования при разработке информационных систем в сфере информационной безопасности;
- использование технологий проектирования при разработке информационных систем в сфере информационной безопасности.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия	Знать: стандарты управления проектами информационных систем; особенности использования жизненного цикла проекта информационных систем; специфику используемой ИС на объекте информатизации
		Уметь: выбирать рекомендуемый стандарт поддержки ЖЦ ПО ИС; формировать характеристики каждого этапа ЖЦ ПО ИС; учитывать специфику используемой ИС на объекте информатизации
		Владеть: соответствующими технологиями в области применения ИС; навыками управления проектом на всех этапах ЖЦ ПО ИС; использовать нормативно-правовую базу соответствующей ИС
ПК-1. Способен организовать моделирование и оценку уязвимости систем защиты информации в государственных информационных системах	ПК-1.2 Формулирует концепции средств и систем информатизации в защищенном исполнении	Знать: концепции средств и систем информатизации в защищенном исполнении; уязвимости систем защиты информации в государственных информационных системах; методы моделирования уязвимости систем защиты информации
		Уметь: формировать базовую концепцию оценки уязвимости систем защиты информации; характеристики уязвимостей систем защиты информации в государственных информационных системах; применять методы моделирования уязвимости систем защиты информации
		Владеть: навыками применения оценки уязвимости систем защиты информации; набором классификаторов уязвимости систем защиты информации; рекомендованными стандартными оценками в области моделирования уязвимости систем защиты информации

ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.1 Проектирует архитектуру автоматизированной системы	Знать: задачи автоматизации; элементы проектирования архитектуры автоматизированных систем; свойства проектирования а автоматизируемой системы
		Уметь: представлять систему в виде набора слабо связанных частей; формировать программные модули, реализующие отдельные функции; применять рекомендуемые специализированные технологии разработки
		Владеть: стандартными технологиями проектирования автоматизированных систем; рекомендуемыми методологиями, ориентированными на предметную область; современными средствами проектирования и разработки автоматизированных систем

3 Общая трудоемкость дисциплины составляет 144 часа, 4 зачетные единицы.

4 Содержание дисциплины

Раздел 1.Жизненный цикл информационной системы (ЖЦ ИС). Модели ЖЦ ИС.

Раздел 2.Методологии и технологии проектирования ИС.

Раздел 3.Инструментальные средства разработки и поддержки ИС.

**Аннотация рабочей программы дисциплины
Б1.В.ДВ.01.02 Структуры и алгоритмы обработки данных**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

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

Задачи дисциплины:

- предоставление теоретических основ по методам и алгоритмам обработки данных;
- освоение навыков по использованию технологий поиска, сортировки, сжатия данных при решении прикладных задач.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-1. Способен организовать моделирование и оценку уязвимости систем защиты информации в государственных информационных системах	ПК-1.2 Формулирует концепции средств и систем информатизации в защищенном исполнении	Знать: концепции средств и систем информатизации в защищенном исполнении; уязвимости систем защиты информации в государственных информационных системах; методы моделирования уязвимости систем защиты информации
		Уметь: формировать базовую концепцию оценки уязвимости систем защиты информации; характеристики уязвимостей систем защиты информации в государственных информационных системах; применять методы моделирования уязвимости систем защиты информации
		Владеть: навыками применения оценки уязвимости систем защиты информации; набором классификаторов уязвимости систем защиты информации; рекомендованными стандартными оценками в области моделирования уязвимости систем защиты информации
ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.1 Проектирует архитектуру автоматизированной системы	Знать: способы проектирования методов обеспечения информационной безопасности для ПО и ИС; методы проектирования обеспечения информационной безопасности для ПО и ИС; способы проектирования обеспечения информационной безопасности для ПО и ИС
		Уметь: организовывать проектирование структур и методов обеспечения информационной безопасности для ПО и ИС; поддерживать проектирование и эксплуатацию структур и методов обеспечения информационной безопасности для ПО и ИС; оформлять результаты проектирования и эксплуатации методов обеспечения информационной безопасности для ПО и ИС
		Владеть: способами организации проектирования и эксплуатации обеспечения информационной безопасности для ПО и ИС; методами обеспечения информационной безопасности для ПО и ИС; методами

3 Общая трудоемкость дисциплины составляет 144 часа, 4 зачетные единицы.

4 Содержание дисциплины

Раздел 1. Структуры данных.

Раздел 2. Методы обработки данных.

Аннотация рабочей программы дисциплины
Б1.В.ДВ.02.01 Инструментарий анализа информационных рисков

1 Цели и задачи дисциплины

Цели преподавания дисциплины:

- раскрытие сущности и значения 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.

Задачи 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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.1 Анализирует и применяет методы анализа информационных рисков в автоматизированных системах	Знать: существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов; механизмы оценки последствий от реализации угроз безопасности
		Уметь: анализировать и оценивать угрозы безопасности при формировании требований пользователя к АС; проводить анализ оценки угроз безопасности информации, с целью повышения эффективности средств и методов ЗИ в АС
		Владеть: методологией анализа информационных рисков; методикой оценки угроз ИБ; навыками выявлять уязвимости в основных компонентах АС и разрабатывать мероприятия по их устранению; способностью оценивать последствия от реализации угроз безопасности информации в автоматизированной системе

3 Общая трудоемкость дисциплины составляет 180 часов, 5 зачетных единиц.

4 Содержание дисциплины

Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.

Раздел 2. Основные этапы и элементы управления рисками и их оценки.

Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.

Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.

**Аннотация рабочей программы дисциплины
Б1.В.ДВ.02.02 Виртуальные частные сети**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

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

Задачи дисциплины:

- ознакомление с понятиями в области криптографических протоколов и стандартов;
- изучение основ построения VPN;
- ознакомление обучающихся с основными практическими приемами построения VPN;
- рассмотрение различных вариантов и схем создания VPN;
- ознакомиться со стандартными протоколами VPN и управлением криптографическими ключами в VPN.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.1 Анализирует и применяет методы анализа информационных рисков в автоматизированных системах	Знать: существующие методические подходы к оценке информационных рисков и основные тенденции развития систем информационной рискозащищенности хозяйствующих субъектов; механизмы оценки последствия от реализации угроз безопасности; механизмы построения VPN и методы защиты внутренней сети с помощью VPN-протоколов
		Уметь: анализировать и оценивать угрозы безопасности при формировании требований пользователя к автоматизированной системе (АС); проводить анализ оценки угроз безопасности информации с целью повышения эффективности средств и методов ЗИ в АС и дальнейшим построением и внедрением VPN
		Владеть: методологией анализа информационных рисков; методикой оценки угроз информационной безопасности; навыками выявлять уязвимости в основных компонентах АС и разрабатывать мероприятия по их устранению с помощью VPN-протоколов; способностью оценивать последствия от реализации угроз безопасности информации в автоматизированной системе через VPN

3 Общая трудоемкость дисциплины составляет 180 часов, 5 зачетных единиц.

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.03.01 Защита в государственных информационных системах

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- формирование знаний и навыков в области реализации системы защиты информации в государственных информационных системах.

Задача 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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-1. Способен организовать моделирование и оценку уязвимости систем защиты информации в государственных информационных системах	ПК-1.1 Выполняет моделирование и оценку угроз систем защиты информации в государственных информационных системах	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; принципы построения средств защиты информации
		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; оценивать эффективность защиты информации
		Владеть: навыками работы со средствами защиты информации от несанкционированного доступа и средствами криптографической защиты информации

3 Общая трудоемкость дисциплины составляет 216 часов, 6 зачетных единиц.

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.03.02 Методология определения ценности информации**

1 Цели и задачи дисциплины

Цель преподавания 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.

Задача 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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-1. Способен организовать моделирование и оценку уязвимости систем защиты информации в государственных информационных системах	ПК-1.1 Выполняет моделирование и оценку угроз систем защиты информации в государственных информационных системах	<p>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; принципы построения программно-аппаратных средств защиты информации; классификацию видов, методов и средств защиты информации</p> <p>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 выработать 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; оценивать эффективность защиты информации</p>

		Владеть: методами определения ценности информации; специальной профессиональной терминологией; основными экономическими методами защиты информации
--	--	--

3 Общая трудоемкость дисциплины составляет 216 часов, 6 зачетных единиц.

4 Содержание дисциплины

Раздел 1. Теория экономики защиты информации

Раздел 2. Защита информации в производственно-хозяйственной деятельности.

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

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

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

Задачи дисциплины:

- изучение защитных механизмов добавочных (наложенных) ПАСЗИ;
- получение практических навыков администрирования добавочных ПАСЗИ;
- анализ рынка современных программно-аппаратных средств защиты информации.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.2 Исследует архитектуру системы защиты информации для оценки функциональных возможностей добавочных программно-аппаратных средств защиты информации	Знать: методику проведения аудита информационной безопасности с точки зрения оценки уровня защищенности объекта; возможности и способы использования безопасных информационных технологий при практической эксплуатации ПАСЗИ
		Уметь: проводить выбор добавочных ПАСЗИ с целью обеспечения требуемого уровня защищенности
		Владеть: способностью организовать выполнение работ по вводу в эксплуатацию ПАСЗИ
ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.2 Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации	Знать: состав компонент и функции добавочных ПАСЗИ от несанкционированного доступа (НСД) и утечек информации
		Уметь: применять в различных проектах программно-аппаратные средства обеспечения информационной безопасности; администрировать ПАСЗИ
		Владеть: навыками выполнения работ по настройке ПАСЗИ

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

4 Содержание дисциплины

Раздел 1. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их технологические особенности, взаимодействие с общесистемными компонентами автоматизированных систем.

Раздел 2. Система защиты SecretNetStudio. DLP-системы. SIEM- системы.

**Аннотация рабочей программы дисциплины
Б1.В.ДВ.04.02 Криптографические протоколы**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- изучение криптографических протоколов.

Задача дисциплины:

- освоение методов анализа криптопротоколов, основных сфер практического применения и особенностей реализации.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.2 Исследует архитектуру системы защиты информации для оценки функциональных возможностей добавочных программно-аппаратных средств защиты информации	Знать: виды атак на криптопротоколы; способы анализа криптографических протоколов
		Уметь: 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
ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.2 Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации	Знать: основные классы криптографических протоколов
		Уметь: оценивать функциональные возможности криптопротоколов
		Владеть: навыками администрирования продуктов на базе криптографических протоколов

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

4 Содержание дисциплины

Раздел 1. Понятие криптографического протокола. Классификация криптографических протоколов. Формальные методы анализа протоколов обеспечения безопасности

Раздел 2. Протоколы идентификации и аутентификации. Протоколы, использующие технику доказательства знания. Протоколы передачи ключей. Протокол TLS/SSL

Аннотация рабочей программы практики
Б2.О.01(П) Производственная - предметно-ознакомительная практика

1 Цели и задачи прохождения практики

Цели прохождения практики:

- получение первичных профессиональных знаний;
- закрепление, развитие и совершенствование первичных теоретических знаний, полученных обучающимися в процессе обучения;
- приобретение профессиональных навыков и умений работы со специализированным оборудованием.

Задачи практики:

- проверка и закрепление полученных теоретических знаний;
- профессиональная ориентация обучающихся, формирование у них полного представления о своей профессии;
- ознакомление с нормативно-правовыми актами, приказами, распоряжениями, указаниями и инструкциями, регламентирующими деятельность в области информационной безопасности;
- приобретение знаний о работе со специализированным оборудованием;
- приобретение навыков профессионального общения при проведении работ в области информационной безопасности;
- сбор материалов, необходимых для составления отчета о практике;
- подготовка обучающихся к осознанному и углубленному изучению обще профессиональных и специальных дисциплин.

2 Требования к результатам прохождения практики

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	УК-1.1 Анализирует проблемную ситуацию, определяет причины ее возникновения и осуществляет её декомпозицию на отдельные задачи	Знать: нормативно-правовые источники и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
		Уметь: анализировать проблемную ситуацию, определять причины ее возникновения и осуществлять её декомпозицию на отдельные задачи
		Владеть: навыками по анализу проблемной ситуации, определять причины ее возникновения и осуществлять её декомпозицию на отдельные задачи
	УК-1.2 Вырабатывает стратегию достижения поставленной цели	Знать: основные стратегии для достижения поставленных целей
		Уметь: выработать стратегии для достижения целей
		Владеть: навыками по созданию стратегий по достижению поставленных целей

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

4 Содержание практики

Раздел 1. Подготовительный этап: получение задания на практику, прохождение инструктажа по пожарной безопасности и технике безопасности и, если нужно, медицинского осмотра.

Раздел 2. Основной этап: выполнение индивидуального задания на практику.

Раздел 3. Подготовка отчета по практике: написание отчета по практике в соответствии с утвержденными в университете требованиями. Защита отчета руководителю практики от университета.

Аннотация рабочей программы практики
Б2.О.02(Н) Производственная - научно-исследовательская работа

1 Цели и задачи прохождения практики

Цели прохождения 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 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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	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; особенности функционирования программных средств с целью выявления потенциальных уязвимостей систем защиты информации
		Уметь: анализировать и обрабатывать полученных в результате практики данных; оформить результаты практики в соответствии с требованиями и стандартами для научно-технической документации; окончательно сформулировать тему исследования и обосновать целесообразность ее разработки
	Владеть: навыками по систематизации и обобщении научной информации по теме исследований; навыками по теоретическому, программно-аппаратному исследованию в рамках выявления потенциальных уязвимостей систем защиты информации автоматизированных систем; навыками анализа научной и практической значимости проводимых исследований	
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет	Знать: функциональные возможности компонентов автоматизированных систем с целью выявления уязвимостей систем защиты информации автоматизированных систем; правила эксплуатации оборудования, применяемого при обеспечении ИБ;

	использовать эти знания в при решении поставленных задач	требования и стандарты по оформлению научно-технической документации
		Уметь: применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение из профессиональной области; использовать функциональные возможности компонентов автоматизированных систем с целью выявления уязвимостей систем
		Владеть: навыками рационального использования функциональных возможностей компонентов автоматизированных систем; оценки достоверности и значимости полученных результатов; навыками использования функциональных возможностей компонентов автоматизированных систем с целью выявления уязвимостей систем

3 Общая трудоемкость практики составляет 432 часа, 12 зачетных единиц.

4 Содержание практики

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.

**Аннотация рабочей программы практики
Б2.О.03(П) Производственная - проектная практика**

1 Цели и задачи прохождения практики

Цели прохождения практики:

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

- развитие практических умений планировать систему защиты.

Задачи практики:

- уметь систематизировать и обобщить научную информацию по теме исследований;

- знать методику анализа угроз информационной безопасности (ИБ) и уязвимостей в информационной системе (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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия	Знать: процедуру анализа полученных теоретических знаний для обеспечения ИБ информационных систем или объектов; литературные и интернет- источники по разрабатываемой теме с целью их использования при составлении планов по обеспечению ИБ; план теоретических и экспериментальных работ; 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; применить и эксплуатировать оборудование, применяемое при обеспечении ИБ; анализировать и обрабатывать полученные в результате практики данные
		Владеть: навыками по систематизации и обобщении научной информации по теме исследований; навыками оценки достоверности и значимости полученных результатов; навыками особенности создания защищенных ИС; навыками анализа угроз ИБ и уязвимостей в ИС
	УК-2.2 Осуществляет эффективное управление проектом на всех этапах жизненного цикла для достижения конечного результата	Знать: 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: применить информационные технологии в научных исследованиях и необходимое программные и техническое обеспечение; оформить результаты практики в

		соответствии с требованиями и стандартами для научно-технической документации
		Владеть: навыками планирования и проектирования систем обеспечения ИБ; навыками использования программно-аппаратных средств обеспечения информационной безопасности ИС; навыками анализа научной и практической значимости проводимых исследований
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты	Знать: современную нормативную базу в области ИБ; программы (регламент) проведения аудита ИБ объекта информатизации
		Уметь: принимать участие в проведении аудита ИБ объекта информатизации
		Владеть: инструментарием проведения аудита ИБ объекта информатизации
	ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ	Знать: порядок разработки проекта компонента комплексной защиты информации
		Уметь: оформлять результаты предпроектного обследования объектов информатизации
		Владеть: навыками критического анализа результатов предпроектного обследования

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

4 Содержание практики

Раздел 1. Подготовительный этап: противопожарный инструктаж и инструктаж по технике безопасности; получение указаний по прохождению практики.

Раздел 2. Основной этап: анализ предметной области (деятельности предприятия, аудит ИБ, выяснение проблем и т.п.); выявление особенности создания защищенных ИС; анализ угроз ИБ и уязвимостей в ИС; развитие навыков планирования и проектирования систем обеспечения ИБ; составление плана работ и примерного проекта системы защиты объекта; проведение исследования отдельных проблем ИБ.

Раздел 3. Подготовка отчета по практике; защита отчета научному руководителю (дифференцированный зачет).

Аннотация программы БЗ Государственная итоговая аттестация

1 В программу государственной итоговой аттестации входят:

БЗ.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы;

БЗ.02(Д) Защита выпускной квалификационной работы.

2 Цели и задачи государственной итоговой аттестации

Цели государственной итоговой аттестации:

- 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 Безопасность информационных систем и технологий;

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

Задачи государственной итоговой аттестации:

- определение уровня теоретической и практической подготовки выпускников по направлению подготовки 10.04.01 Безопасность информационных систем и технологий;

- определение степени владения и умения обучающимися применять знания, умения и навыки для решения профессиональных задач;

- разработка стратегии проектирования, определение целей проектирования, критериев эффективности, ограничений применимости;

- концептуальное проектирование средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

- подготовка организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

- выбор и внедрение в практику систем и средств обеспечения информационной безопасности;

- унификация и типизация проектных решений;

- авторское сопровождение процессов проектирования, внедрения и сопровождения систем и средств обеспечения информационной безопасности на производстве.

3 Требования к результатам прохождения государственной итоговой аттестации

Перечень компетенций, выносимых на выполнение выпускной квалификационной работы:

Универсальные компетенции выпускников и индикаторы их достижения		
Категория универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию, определяет причины ее возникновения и осуществляет её декомпозицию на отдельные задачи
		УК-1.2 Вырабатывает стратегию достижения поставленной цели
Разработка и реализация проектов	УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия

		УК-2.2 Осуществляет эффективное управление проектом на всех этапах жизненного цикла для достижения конечного результата
Командная работа и лидерство	УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Демонстрирует понимание принципов командной работы
		УК-3.2 Ставит задачи перед членами команды, руководит ими для достижения поставленной задачи
Коммуникация	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 Способен к устной и письменной коммуникации по профессионально релевантным темам на иностранном языке
		УК-4.2 Способен к извлечению информации из отечественных и зарубежных источников научного характера с последующей переработкой (компрессией) в виде обзора, аннотации, реферата, доклада, презентации на иностранном языке
		УК-4.3 Использует информационно-коммуникационные технологии для поиска, обработки и представления информации
		УК-4.4 Представляет результаты академической и профессиональной деятельности на публичных мероприятиях
Межкультурное взаимодействие	УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Демонстрирует понимание особенностей различных культур
		УК-5.2 Выстраивает социальное взаимодействие, учитывая общее и особенное различных культур
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания
		УК-6.2 Определяет приоритеты личностного роста и способы совершенствования собственной деятельности на основе самооценки и самообучения

Общепрофессиональные компетенции выпускников и индикаторы их достижения		
Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Категория отсутствует	ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты
		ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ
Категория отсутствует	ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1 Знает требования к оформлению технического проекта системы обеспечения ИБ и особенности его разработки
		ОПК-2.2 Умеет разрабатывать технический проект системы ИБ, выбирать технологии защиты

		обеспечивающей части информационно-аналитической системы (ИАС)
Категория отсутствует	ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает основные виды организационно-распорядительных документов в области ИБ, требования по формированию политик ИБ, защите компьютерных систем и сетей
		ОПК-3.2 Умеет разрабатывать организационно-распорядительные документы и формировать политику в области информационной безопасности
Категория отсутствует	ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ
		ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач
Категория отсутствует	ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1 Знает порядок проведения и особенности исследований в области информационной безопасности, требования к оформлению научной и деловой документации
		ОПК-5.2 Умеет решать прикладные задачи с использованием современных информационных технологий, готовить доклады и отчёты по выполненной работе

Профессиональные компетенции выпускников и индикаторы их достижения				
Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: организационно-управленческий				
Организационно-управленческие работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации,	Системы комплексы средств управления информационной безопасностью компьютерных систем; информационные технологии, формирующие информационную инфраструктуру, в условиях существования угроз в информационной сфере и задействующие информационные ресурсы,	ПК-1. Способен организовать моделирование и оценку уязвимости систем защиты информации в государственных информационных системах	ПК-1.1 Выполняет моделирование и оценку угроз систем защиты информации в государственных информационных системах	06.033 - Специалист по защите информации в автоматизированных системах
			ПК-1.2 Формулирует концепции средств и систем информатизации в защищенном исполнении	06.033 - Специалист по защите информации в автоматизированных системах

<p>Федеральной службы по техническому и экспортному контролю Российской Федерации; организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организационно-правовые механизмы обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, стандартизации, сертификации и контроля качества защиты информации и информационных ресурсов.</p>	<p>подлежащие защите.</p>			
<p>Тип задач профессиональной деятельности: научно-исследовательский</p>				
<p>Организационно-управленческие работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной</p>	<p>Системы комплексы средств управления информационной безопасностью компьютерных систем; информационные технологии, формирующие информационную инфраструктуру, в условиях существования угроз в информационной сфере и действующие информационные ресурсы,</p>	<p>ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты</p>	<p>ПК-2.1 Анализирует и применяет методы анализа информационных рисков в автоматизированных системах</p> <p>ПК-2.2 Исследует архитектуру системы защиты информации для оценки функциональных возможностей добавочных программно-аппаратных средств защиты информации</p>	<p>06.033 - Специалист по защите информации в автоматизированных системах</p> <p>06.033 - Специалист по защите информации в автоматизированных системах</p>

<p>службы по техническому и экспортному контролю Российской Федерации; организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организационно-правовые механизмы обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, стандартизации, сертификации и контроля качества защиты информации и информационных ресурсов.</p>	<p>подлежащие защите.</p>			
<p>Тип задач профессиональной деятельности: проектный</p>				
<p>Разработка и исследование экспериментальных моделей, обработка результатов исследований. Проведение исследований в области информационной безопасности, изучение требований к оформлению научной и деловой документации. Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности.</p>	<p>Технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта).</p>	<p>ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности</p>	<p>ПК-3.1 Проектирует архитектуру автоматизированной системы ПК-3.2 Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации</p>	<p>06.033 - Специалист по защите информации в автоматизированных системах 06.033 - Специалист по защите информации в автоматизированных системах</p>

Перечень компетенций, выносимых на защиту выпускных квалификационных работ:

Универсальные компетенции выпускников и индикаторы их достижения		
Категория универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию, определяет причины ее возникновения и осуществляет её декомпозицию на отдельные задачи
		УК-1.2 Вырабатывает стратегию достижения поставленной цели
Разработка и реализация проектов	УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Участвует в формировании структуры (стадий и этапов) жизненного цикла изделия
		УК-2.2 Осуществляет эффективное управление проектом на всех этапах жизненного цикла для достижения конечного результата
Командная работа и лидерство	УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Демонстрирует понимание принципов командной работы
		УК-3.2 Ставит задачи перед членами команды, руководит ими для достижения поставленной задачи
Коммуникация	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 Способен к устной и письменной коммуникации по профессионально релевантным темам на иностранном языке
		УК-4.2 Способен к извлечению информации из отечественных и зарубежных источников научного характера с последующей переработкой (компрессией) в виде обзора, аннотации, реферата, доклада, презентации на иностранном языке
		УК-4.3 Использует информационно-коммуникационные технологии для поиска, обработки и представления информации
		УК-4.4 Представляет результаты академической и профессиональной деятельности на публичных мероприятиях
Межкультурное взаимодействие	УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Демонстрирует понимание особенностей различных культур
		УК-5.2 Выстраивает социальное взаимодействие, учитывая общее и особенное различных культур
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания
		УК-6.2 Определяет приоритеты личностного роста и способы совершенствования собственной деятельности на основе самооценки и самообучения

Общепрофессиональные компетенции выпускников и индикаторы их достижения		
Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции

Категория отсутствует	ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Знает порядок проведения предпроектного обследования объектов информатизации, средства и особенности их защиты
		ОПК-1.2 Умеет оформить результаты предпроектного обследования объектов информатизации в виде требований на создание системы обеспечения ИБ
Категория отсутствует	ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1 Знает требования к оформлению технического проекта системы обеспечения ИБ и особенности его разработки
		ОПК-2.2 Умеет разрабатывать технический проект системы ИБ, выбирать технологии защиты обеспечивающей части информационно-аналитической системы (ИАС)
Категория отсутствует	ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает основные виды организационно-распорядительных документов в области ИБ, требования по формированию политик ИБ, защите компьютерных систем и сетей
		ОПК-3.2 Умеет разрабатывать организационно-распорядительные документы и формировать политику в области информационной безопасности
Категория отсутствует	ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ
		ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач
Категория отсутствует	ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1 Знает порядок проведения и особенности исследований в области информационной безопасности, требования к оформлению научной и деловой документации
		ОПК-5.2 Умеет решать прикладные задачи с использованием современных информационных технологий, готовить доклады и отчеты по выполненной работе

Профессиональные компетенции выпускников и индикаторы их достижения

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: организационно-управленческий				
Организационно-управленческие работы по созданию или	Системы комплексы средств управления информационной безопасностью	ПК-1 Способен организовать моделирование и оценку уязвимости	ПК-1.1 Выполняет моделирование и оценку угроз систем защиты	06.033 - Специалист по защите информации в

<p>модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации; организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; организационно-правовые механизмы обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, стандартизации, сертификации и контроля качества защиты информации и информационных ресурсов</p>	<p>компьютерных систем; информационные технологии, формирующие информационную инфраструктуру, в условиях существования угроз в информационной сфере и задействующие информационные ресурсы, подлежащие защите</p>	<p>систем защиты информации в государственных информационных системах</p>	<p>информации в государственных информационных системах</p>	<p>автоматизированных системах</p>
			<p>ПК-1.2 Формулирует концепции средств и систем информатизации в защищенном исполнении</p>	<p>06.033 - Специалист по защите информации в автоматизированных системах</p>
<p>Тип задач профессиональной деятельности: научно-исследовательский</p>				
<p>Разработка и исследование экспериментальных моделей, обработка</p>	<p>Технологии обеспечения информационной безопасности объектов</p>	<p>ПК-2 Способен организовать работы по выявлению недостатков в</p>	<p>ПК-2.1 Анализирует и применяет методы анализа информационных</p>	<p>06.033 - Специалист по защите информации в автоматизированных системах</p>

результатов исследований. Проведение исследований в области информационной безопасности, изучение требований к оформлению научной и деловой документации. Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности	различного уровня (система, объект системы, компонент объекта)	функционировании системы защиты	рисков в автоматизированных системах	06.033 - Специалист по защите информации в автоматизированных системах
			ПК-2.2 Исследует архитектуру системы защиты информации для оценки функциональных возможностей добавочных программно-аппаратных средств защиты информации	
Тип задач профессиональной деятельности: проектный				
Разработка проектов в сфере информационной безопасности, подготовка организационно-распорядительной, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности. Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации	Компьютерные, автоматизированные, информационные и информационно-аналитические системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите	ПК-3 Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.1 Проектирует архитектуру автоматизированной системы	06.033 - Специалист по защите информации в автоматизированных системах
			ПК-3.2 Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации	06.033 - Специалист по защите информации в автоматизированных системах

4 Общая трудоемкость государственной итоговой аттестации составляет 324 часа, 9 зачетных единиц.

5 Содержание государственной итоговой аттестации

Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы: Изучение литературы и иных источников по проблеме, определение целей, задач и методов исследования; непосредственная разработка проблемы (темы), выполнение теоретических и прикладных исследований; обобщение и оценка полученных результатов исследования (работы); написание и оформление ВКР.

Б3.02(Д) Защита выпускной квалификационной работы: Рецензирование работы; подготовка к защите ВКР; защита и оценка работы.

Процедура оценивания результатов защиты ВКР состоит из следующих этапов: Этап 1. Оценка уровня сформированности компетенций по результатам теоретического обучения обучающегося – определяется как среднее арифметическое оценок (с точностью до десятых долей), полученных по всем дисциплинам и практикам, в том числе НИР, предусмотренным учебным планом. Этап 2. Оценка публичной защиты обучающимся ВКР в соответствии с показателям и критериям. Этап 3. Оценка ВКР рецензентом. Этап 4. Оценка ВКР руководителем. Этап 5. Оценка результатов освоения образовательной программы обучающимся определяется как среднее арифметическое оценок, перечисленных в первых четырех пунктах данных методических материалов. Этап 6. Итоговая оценка публичной защиты ВКР – оценка, идущая в приложение к диплому, – это оценка результатов освоения образовательной программы обучающимся, округленная до ближайшего целого значения.

**Аннотация рабочей программы дисциплины
ФТД.01 Интеллектуальные информационные системы**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- сформировать представления о месте и роли искусственного интеллекта (ИИ) в задачах информационной безопасности (ИБ).

Задачи дисциплины:

- познакомить с основными технологиями ИИ;
- ознакомить с возможностями и перспективами создания систем информатизации в защищённом исполнении на основе технологий ИИ.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	Знать: основные задачи ИИ и методы их решения
		Уметь: выявлять задачи ИБ, решаемые на основе технологий ИИ
		Владеть: представлением о возможностях защиты ИС на основе технологий ИИ
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач	Знать: основные возможности технологий ИИ в задачах ИБ
		Уметь: работать с литературой по методам ИИ в области ИБ
		Владеть: представлением о возможностях защиты ИС на основе технологий ИИ

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

4 Содержание дисциплины

Раздел 1 История и задачи.

Раздел 2 Основные технологии и методы ИИ в ИБ.

Раздел 3 Применение ИИ для создания ИС в защищённом исполнении.

**Аннотация рабочей программы дисциплины
ФТД.02 Корпоративные информационные системы**

1 Цели и задачи дисциплины

Цель преподавания дисциплины:

- сформировать представления о месте и роли проблем информационной безопасности (ИБ) в области корпоративных информационных систем (КИС).

Задачи дисциплины:

- познакомить с основными классами КИС, особенностями их разработки и эксплуатации с точки зрения ИБ;
- ознакомить с проблемами разработки КИС в защищённом исполнении.

2 Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1 Знает основные направления и тенденции развития технологий в области ИБ	Знать: основные виды КИС; основные проблемы и методы обеспечения ИБ КИС
		Уметь: анализировать проблемы КИС с точки зрения задач ИБ
		Владеть: представлением о безопасности КИС как элемента критической информационной инфраструктуры (КИИ)
	ОПК-4.2 Умеет осуществлять сбор, обработку и анализ современной научно-технической информации в области информационной безопасности, умеет использовать эти знания в при решении поставленных задач	Знать: особенности функционирования КИС с позиции ИБ
Уметь: работать с литературой по проблемам ИБ для критической информационной инфраструктуры (КИИ)		
Владеть: представлением о роли КИС как элемента критической информационной инфраструктуры (КИИ)		

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

4 Содержание дисциплины

Раздел 1 Введение в КИС.

Раздел 2 КИС как открытая система. Сетевые технологии в разработке КИС. Безопасность КИС.

Раздел 3 КИС и КИИ.