



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
Институт кибербезопасности и цифровых технологий

УТВЕРЖДАЮ

И.о. директора ИКБ

_____ Бакаев А.А.

« ____ » _____ 2025 г.

Рабочая программа практики
Производственная практика
Технологическая практика

Читающее подразделение **кафедра КБ-4 «Интеллектуальные системы информационной безопасности»**
Направление **10.04.01 Информационная безопасность**
Направленность **Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта**
Квалификация **магистр**
Форма обучения **очная**
Общая трудоемкость **11 з.е.**

Распределение часов дисциплины и форм промежуточной аттестации по семестрам

Семестр	Зачётные единицы	Распределение часов							Формы промежуточной аттестации
		Всего	Лекции	Лабораторные	Практические	Самостоятельная работа	Контактная работа в период практики и (или) аттестации	Контроль	
3	11	396	0	0	0	370,92	7,33	17,75	Зачет с оценкой
из них на практ. подготовку			0	0	0	185	0	0	

Программу составил(и):

д-р техн. наук, профессор, Козьминых С.И. _____

Рабочая программа практики

Технологическая практика

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 10.04.01 Информационная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1455)

составлена на основании учебного плана:

направление: 10.04.01 Информационная безопасность

направленность: «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Рабочая программа одобрена на заседании кафедры

кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Протокол от 24.01.2025 № 6

Зав. кафедрой Максимова Е.А. _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры

кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Протокол от _____ 2026 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры

кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Протокол от _____ 2027 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры

кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Протокол от _____ 2028 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029-2030 учебном году на заседании кафедры

кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Протокол от _____ 2029 г. № ____

Зав. кафедрой _____
Подпись _____ Расшифровка подписи _____

1. ЦЕЛИ ОСВОЕНИЯ ПРАКТИКИ

«Технологическая практика» имеет своей целью сформировать, закрепить и развить практические навыки и компетенции, предусмотренные данной рабочей программой в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки – «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта».

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Направление:	10.04.01 Информационная безопасность
Направленность:	Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта
Блок:	Практика
Часть:	Обязательная часть
Общая трудоемкость:	11 з.е. (396 акад. час.).

3. ТИП, ВИД И СПОСОБ ПРОВЕДЕНИЯ ПРАКТИКИ

Вид практики:	Производственная практика
Тип практики:	Технологическая практика

Способ (способы) проведения практики определяются в соответствии с федеральным государственным образовательным стандартом. В случае, если стандарт не регламентирует способ проведения практики, то она проводится стационарно.

4. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ ПРАКТИКИ

«Технологическая практика» направления подготовки 10.04.01 Информационная безопасность проводится на базе структурных подразделений РТУ МИРЭА или в организации, осуществляющей деятельность по профилю соответствующей образовательной программы (далее - профильная организация), в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора, заключаемого между образовательной организацией и профильной организацией.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ

В результате освоения практики обучающийся должен овладеть компетенциями:

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

УК-3 - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ИИ-ОПК-1 - Способен адаптировать и применять на практике классические и новые научные принципы и методы исследований для решения задач в области создания и применения технологий и систем искусственного интеллекта и методы исследований

ИИ-ОПК-2 - Способен использовать методы научных исследований и математического моделирования в области проектирования и управления системами искусственного интеллекта

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, ХАРАКТЕРИЗУЮЩИЕ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

УК-2 : Способен управлять проектом на всех этапах его жизненного цикла

УК-2.1 : Разрабатывает концепцию проекта в рамках обозначенной проблемы и план реализации проекта с учётом возможных рисков реализации и возможностей их устранения

Знать:

- принципы постановки проектной задачи и этапы планирования проектной деятельности

Уметь:

- формулировать проектную задачу и планировать собственную деятельность в рамках реализации проекта

Владеть:

- навыками постановки проектной задачи, способностью планирования своей работы над проектом

УК-2.2 : Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта

Знать:

- этапы, методы и инструменты разработки плана реализации проекта

Уметь:

- разрабатывать план реализации проекта с учётом целей, ресурсов, сроков и рисков

Владеть:

- навыками разработки плана реализации проекта

УК-3 : Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

УК-3.1 : Вырабатывает стратегию командной работы и на её основе организует отбор членов команд для достижения поставленной цели

Знать:

- принципы и подходы к формированию стратегии командной работы в проектной деятельности

Уметь:

- разрабатывать и адаптировать стратегию командного взаимодействия для эффективного достижения целей проекта

Владеть:

- навыками выработки стратегии командной работы

УК-3.2 : Руководит работой команды, разрешает противоречия на основе учёта интереса всех сторон

Знать:

- основы организации командной работы и принципы эффективного взаимодействия в коллективе

Уметь:

- организовывать командную деятельность с учётом целей проекта, распределения ролей и

сроков выполнения задач

Владеть:

- навыками организации командной работы

ОПК-1 : Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-1.1 : Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении

Знать:

- отечественные и зарубежные стандарты в области информационной безопасности, применяемые при формировании требований технического задания

Уметь:

- использовать стандарты информационной безопасности для разработки требований к техническому заданию

Владеть:

- отечественными и зарубежными стандартами в области информационной безопасности при формировании требований технического задания

ОПК-1.2 : Проектирует информационные системы с учетом технологий обеспечения информационной безопасности

Знать:

- инструменты и методы проектирования информационных систем с учетом требований информационной безопасности

Уметь:

- применять инструменты проектирования информационных систем с интеграцией технологий обеспечения информационной безопасности

Владеть:

- инструментами проектирования информационных систем с учетом технологий обеспечения информационной безопасности

ОПК-1.3 : Формирует актуальные модели угроз и нарушителей для автоматизированных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности

Знать:

- актуальные модели угроз для автоматизированных информационных систем и подходы к оценке эффективности систем информационной безопасности

Уметь:

- применять актуальные модели угроз и разрабатывать критерии оценки эффективности проектируемых систем информационной безопасности

Владеть:

- актуальными моделями угроз для автоматизированных информационных систем, владеет инструментами разработки и обоснования критериев оценки эффективности проектируемой системы обеспечения информационной безопасности

ОПК-2 : Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

ОПК-2.1 : Применяет методы концептуального проектирования технологий обеспечения информационной безопасности

Знать:

- методы и принципы концептуального проектирования технологий обеспечения информационной безопасности

Уметь:

- применять методы концептуального проектирования при разработке технологий защиты информации

Владеть:

- методами концептуального проектирования технологий обеспечения информационной безопасности

ОПК-2.2 : Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью

Знать:

- методы и средства защиты информации в компьютерных системах и сетях, а также критерии их обоснованного выбора

Уметь:

- обоснованно выбирать и применять методы решения задач по обеспечению защиты информации в компьютерных системах и сетях

Владеть:

- способностью обоснованно выбирать и применять методы решения задач для защиты информации компьютерных систем и сетей

ОПК-2.3 : Выполняет работы по защите информации при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности

Знать:

- классификацию, принципы действия и область применения инструментов и методов защиты информации

Уметь:

- выбирать и применять соответствующие инструменты и методы для защиты информации в зависимости от типа угроз и задач

Владеть:

- инструментами и методами по защите информации

ОПК-3 : Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ОПК-3.1 : Применяет отечественные стандарты при сертификации средств защиты и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки организационно-распорядительных документов

Знать:

- отечественные стандарты и нормативно-правовые акты, регламентирующие сертификацию средств защиты информации и аттестацию объектов информатизации

Уметь:

- применять отечественные стандарты при подготовке и проведении сертификации средств защиты и аттестации объектов информатизации

Владеть:

- отечественными стандартами при сертификации средств защиты и аттестации объектов информатизации

ОПК-3.2 : Разрабатывает технические задания на создание подсистем обеспечения информационной безопасности

Знать:

- требования к структуре, содержанию и оформлению технического задания на создание подсистем информационной безопасности

Уметь:

- разрабатывать техническое задание на проектирование и внедрение подсистем информационной безопасности с учетом нормативных требований

Владеть:

- разработкой технического задания на создание подсистем информационной безопасности

ОПК-3.3 : Исследует эффективность и проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности

Знать:

- цели, этапы и методы технико-экономического обоснования проектных решений в области построения систем информационной безопасности

Уметь:

- проводить технико-экономическое обоснование проектных решений с учетом требований безопасности, затрат и эффективности

Владеть:

- способами проведения технико-экономического обоснования проектных решений в области построения систем обеспечения информационной безопасности

ИИ-ОПК-1 : Способен адаптировать и применять на практике классические и новые научные принципы и методы исследований для решения задач в области создания и применения технологий и систем искусственного интеллекта и методы исследований

ИИ-ОПК-1.1 : Адаптирует известные научные принципы и методы исследований с целью их практического применения

Знать:

- существующие математические, естественно-научные и социально-экономические методы, применяемые при создании и использовании систем искусственного интеллекта

Уметь:

- адаптировать математические, естественно-научные и социально-экономические методы для решения типовых и нестандартных задач в области искусственного интеллекта

Владеть:

- способностью адаптировать существующие математические, естественно-научные и социально экономические методы для решения основных, нестандартных задач создания и применения искусственного интеллекта

ИИ-ОПК-1.2 : Решает профессиональные задачи на основе применения новых научных принципов и методов исследования

Знать:

- основные и нестандартные задачи, возникающие при создании и применении систем искусственного интеллекта, а также подходы к их решению

Уметь:

- решать основные и нестандартные задачи, связанные с разработкой, внедрением и применением технологий искусственного интеллекта

Владеть:

- навыками решения основных, нестандартных задач создания и применения искусственного интеллекта

ИИ-ОПК-2 : Способен использовать методы научных исследований и математического моделирования в области проектирования и управления системами искусственного интеллекта

ИИ-ОПК-2.1 : Применяет логические методы и приемы научного исследования, методологические принципы современной науки, направления, концепции, источники знания и приемы работы с ними, основные особенности научного метода познания, программно-целевые методы решения научных проблем в профессиональной деятельности

Знать:

- логические методы и приёмы, применяемые в научном исследовании, их классификацию и область применения

Уметь:

- использовать логические методы и приёмы при формулировании гипотез, анализе результатов и построении научных выводов

Владеть:

- логическими методами и приемами научного исследования

ИИ-ОПК-2.2 : Осуществляет методологическое обоснование научного исследования, создание и применение библиотек искусственного интеллекта

Знать:

- современные информационно-коммуникационные и интеллектуальные компьютерные технологии, а также научные подходы к поиску и обоснованию решений

Уметь:

- осуществлять выбор информационно-коммуникационных и интеллектуальных технологий и применять научную методологию при поиске решений

Владеть:

- способностью осуществлять выбор современных информационно-коммуникационных и интеллектуальных компьютерных технологий, осуществлять поиск решений на основе научной методологии

В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ПРАКТИКИ ОБУЧАЮЩИЙСЯ ДОЛЖЕН

Знать:

- принципы постановки проектной задачи и этапы планирования проектной деятельности
- классификацию, принципы действия и область применения инструментов и методов защиты информации
- методы и принципы концептуального проектирования технологий обеспечения информационной безопасности
- отечественные стандарты и нормативно-правовые акты, регламентирующие сертификацию средств защиты информации и аттестацию объектов информатизации
- актуальные модели угроз для автоматизированных информационных систем и подходы к оценке эффективности систем информационной безопасности
- требования к структуре, содержанию и оформлению технического задания на создание подсистем информационной безопасности
- инструменты и методы проектирования информационных систем с учетом требований информационной безопасности
- цели, этапы и методы технико-экономического обоснования проектных решений в области построения систем информационной безопасности
- существующие математические, естественно-научные и социально-экономические методы, применяемые при создании и использовании систем искусственного интеллекта
- отечественные и зарубежные стандарты в области информационной безопасности, применяемые при формировании требований технического задания
- основные и нестандартные задачи, возникающие при создании и применении систем искусственного интеллекта, а также подходы к их решению
- принципы и подходы к формированию стратегии командной работы в проектной деятельности

- логические методы и приёмы, применяемые в научном исследовании, их классификацию и область применения
- этапы, методы и инструменты разработки плана реализации проекта
- современные информационно-коммуникационные и интеллектуальные компьютерные технологии, а также научные подходы к поиску и обоснованию решений
- основы организации командной работы и принципы эффективного взаимодействия в коллективе
- методы и средства защиты информации в компьютерных системах и сетях, а также критерии их обоснованного выбора

Уметь:

- адаптировать математические, естественно-научные и социально-экономические методы для решения типовых и нестандартных задач в области искусственного интеллекта
- проводить технико-экономическое обоснование проектных решений с учетом требований безопасности, затрат и эффективности
- осуществлять выбор информационно-коммуникационных и интеллектуальных технологий и применять научную методологию при поиске решений
- разрабатывать техническое задание на проектирование и внедрение подсистем информационной безопасности с учетом нормативных требований
- решать основные и нестандартные задачи, связанные с разработкой, внедрением и применением технологий искусственного интеллекта
- применять отечественные стандарты при подготовке и проведении сертификации средств защиты и аттестации объектов информатизации
- выбирать и применять соответствующие инструменты и методы для защиты информации в зависимости от типа угроз и задач
- использовать логические методы и приёмы при формулировании гипотез, анализе результатов и построении научных выводов
- обоснованно выбирать и применять методы решения задач по обеспечению защиты информации в компьютерных системах и сетях
- применять методы концептуального проектирования при разработке технологий защиты информации
- формулировать проектную задачу и планировать собственную деятельность в рамках реализации проекта
- применять актуальные модели угроз и разрабатывать критерии оценки эффективности проектируемых систем информационной безопасности
- разрабатывать план реализации проекта с учётом целей, ресурсов, сроков и рисков
- применять инструменты проектирования информационных систем с интеграцией технологий обеспечения информационной безопасности
- использовать стандарты информационной безопасности для разработки требований к техническому заданию
- разрабатывать и адаптировать стратегию командного взаимодействия для эффективного достижения целей проекта
- организовывать командную деятельность с учётом целей проекта, распределения ролей и сроков выполнения задач

Владеть:

- способностью обоснованно выбирать и применять методы решения задач для защиты информации компьютерных систем и сетей
- логическими методами и приемами научного исследования
- навыками постановки проектной задачи, способностью планирования своей работы над проектом
- навыками решения основных, нестандартных задач создания и применения искусственного интеллекта
- навыками разработки плана реализации проекта

- способностью адаптировать существующие математические, естественно-научные и социально экономические методы для решения основных, нестандартных задач создания и применения искусственного интеллекта
- способами проведения технико-экономического обоснования проектных решений в области построения систем обеспечения информационной безопасности
- методами концептуального проектирования технологий обеспечения информационной безопасности
- навыками организации командной работы
- разработкой технического задания на создание подсистем информационной безопасности
- отечественными и зарубежными стандартами в области информационной безопасности при формировании требований технического задания
- отечественными стандартами при сертификации средств защиты и аттестации объектов информатизации
- инструментами проектирования информационных систем с учетом технологий обеспечения информационной безопасности
- инструментами и методами по защите информации
- актуальными моделями угроз для автоматизированных информационных систем, владеет инструментами разработки и обоснования критериев оценки эффективности проектируемой системы обеспечения информационной безопасности
- навыками выработки стратегии командной работы
- способностью осуществлять выбор современных информационно-коммуникационных и интеллектуальных компьютерных технологий, осуществлять поиск решений на основе научной методологии

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

При проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений и лидерских качеств.

Код занятия	Наименование разделов и тем /вид занятия/	Сем.	Часов
1. 1. Организационный этап			
1.1	Организационное собрание. Инструктаж по технике безопасности и охране труда. Пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда. (КрПА). Индивидуальный план работы. Пройти инструктаж и соблюдать правила техники безопасности, пожарной безопасности и охраны труда. Порядок прохождения практики и правила оформления документов	3	2,67
2. 2. Получение навыков практической деятельности			
2.1	Этап практической деятельности и выполнение индивидуальных заданий (КрПА). Задания на практику	3	1,75
2.2	Выполнение домашнего задания (Ср). Изучение научной литературы по тематике	3	79 (из них 30 на практ. подг.)
2.3	Консультация по практике (КрПА). Консультация по практике	3	2,66

2.4	Выполнение заданий направленных на получение навыков практической подготовки (Ср). Прохождение практики и выполнение работ в соответствии с индивидуальным заданием	3	250 (из них 130 на практ. подг.)
2.5	Анализ информации и формирование отчёта по практической подготовке (Ср). Систематизация и обобщение материалов и оформление отчета по практике	3	41,92 (из них 25 на практ. подг.)
3. Промежуточная аттестация (зачёт с оценкой)			
3.1	Подготовка к сдаче промежуточной аттестации (ЗачётСОц).	3	17,75
3.2	Контактная работа с преподавателем в период промежуточной аттестации (КрПА).	3	0,25

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

7.1. Перечень компетенций

Перечень компетенций, на освоение которых направлена «Технологическая практика», с указанием результатов их формирования в процессе освоения образовательной программы, представлен в п.3 настоящей рабочей программы

7.2. Типовые контрольные вопросы и задания

1. Закон Российской Федерации об образовании
2. Должностные инструкции
3. График работы на неделю
4. Правила оформления отчета
5. Какие Вы знаете приемы анализа профессиональной информации?
6. Какие информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы Вы использовали?
7. Какое современное программное и аппаратное обеспечение информационных и автоматизированных систем Вы использовали?
8. Какие применялись пакеты автоматизированного проектирования и исследований?
9. Какие приемы системной инженерии в области получения, передачи, хранения, переработки и представления информации Вы использовали?
10. Какие методологии управления разработкой программных средств и проектов Вы использовали, почему?
11. Какие компьютерные технологии и соответствующие технические средства Вами использовались?
12. Какие приемы оптимизации совместной работы коллектива исследователей можно было использовать?
13. Какие методики анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий использовались?
14. Законодательные и иные правовые акты в области технической защиты информации
15. Нормативные правовые акты по технической защите информации.
16. Показатели эффективности систем защиты.
17. Методы оценки опасности угроз.
18. Количественный и качественный риск.
19. Какие инструменты и методы защиты информации Вы знаете?
20. Система, подсистема, надсистема.
21. Какие способы проведения технико-экономического обоснования проектных решений в области построения систем обеспечения информационной безопасности Вы знаете?

7.3. Фонд оценочных материалов

Полный перечень оценочных материалов представлен в приложении 1.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Наименование помещения	Перечень основного оборудования
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мультимедийное оборудование, специализированная мебель, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.
Компьютерный класс	Компьютерная техника с возможностью подключения к сети «Интернет», мультимедийное оборудование, специализированная мебель.
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.
Базы практики	Оборудование и технические средства обучения, позволяющем выполнять определенные виды работ, предусмотренные заданием на практику.

8.2. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. P7-Офис.
2. GNU Compiler Collection. Свободное программное обеспечение (лицензия GNU GPL 3)
3. GNU Prolog. Свободное программное обеспечение (лицензия GPL 2)
4. Python. Свободное программное обеспечение (лицензия PSFL)
5. PostgreSQL. Свободное программное обеспечение (лицензия PostgreSQL)
6. LibreOffice. Свободное программное обеспечение (лицензия MPLv2.0)
7. AnyLogic. Свободное программное обеспечение (бесплатная образовательная лицензия)
8. Astra Linux Common Edition релиз "Орел". Лицензия №187711334-ore-2.12-client-3327 от 07.09.2020

8.3. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

8.3.1. Основная литература

1. Нестеров С. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 324 с. — Режим доступа: <https://e.lanbook.com/book/114688>
2. Гаврилова И. В., Масленникова О. Е. Основы искусственного интеллекта [Электронный ресурс]: учеб. пособие. - Москва: ФЛИНТА, 2019. - 283 с. — Режим доступа: <https://e.lanbook.com/book/115839>
3. Колокольцов В. Н., Малафеев О. А. Математическое моделирование многоагентных систем конкуренции и кооперации (Теория игр для всех) [Электронный ресурс]:. - Санкт-Петербург: Лань, 2021. - 624 с. — Режим доступа: <https://e.lanbook.com/book/168398>

4. Приемышев А. В., Крутов В. Н., Треяль В. А., Коршакова О. А. Технологии создания интеллектуальных устройств, подключенных к интернет [Электронный ресурс]:. - Санкт-Петербург: Лань, 2021. - 100 с. – Режим доступа: <https://e.lanbook.com/book/169110>
5. Иванов В. М., Сесекин А. Н. Интеллектуальные системы [Электронный ресурс]: Учебное пособие для вузов. - Москва: Юрайт, 2020. - 91 с – Режим доступа: <https://urait.ru/bcode/453212>
6. Тумбинская М. В., Петровский М. В. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс]: учебник. - Санкт-Петербург: Лань, 2019. - 344 с. – Режим доступа: <https://e.lanbook.com/book/125739>

8.3.2. Дополнительная литература

1. Пенькова Т. Г., Вайнштейн Ю. В. Модели и методы искусственного интеллекта [Электронный ресурс]: учебное пособие. - Красноярск: СФУ, 2019. - 116 с. – Режим доступа: <https://e.lanbook.com/book/157579>
2. Масленникова О. Е., Назарова О. Б., Давлеткиреева Л. З. Теоретические и прикладные основы сопровождения информационных систем [Электронный ресурс]: учебник. - Москва: ФЛИНТА, 2017. - 190 с. – Режим доступа: <https://e.lanbook.com/book/104915>
3. Кривошеин Д. А., Дмитренко В. П., Горькова Н. В. Безопасность жизнедеятельности [Электронный ресурс]: учебное пособие. - Санкт-Петербург: Лань, 2019. - 340 с. – Режим доступа: <https://e.lanbook.com/book/115489>

8.4. РЕКОМЕНДУЕМЫЙ ПЕРЕЧЕНЬ СОВРЕМЕННЫХ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Информационно-правовой портал ГАРАНТ [http:// www.garant.ru](http://www.garant.ru)
2. Консультант Плюс [http:// www.consultant.ru](http://www.consultant.ru)
3. Российский фонд фундаментальных исследований <https://www.rfbr.ru>
4. Научная электронная библиотека <http://www.elibrary.ru>
5. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru>

8.5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ПРАКТИКИ

На первом организационном собрании необходимо ознакомить студентов с содержанием рабочей программы практики, с порядком и графиком прохождения практики.

В начале прохождения практики, на организационно-подготовительном этапе студентам необходимо:

- оформить задание на практику;
- пройти инструктаж по технике безопасности и противопожарной технике;
- ознакомиться с содержанием рабочей программы практики, правилами и обязанностями практиканта на предприятии, структурой подразделений (рабочих мест) практики, режимом работы предприятия;
- ознакомиться со структурой заключительного отчета по практике.

За период прохождения производственной практики студент самостоятельно изучает документацию, связанную с будущей профессиональной деятельностью, учебную, справочную, нормативную и научно-техническую литературу по соответствующим разделам данной программы. Литература подбирается в библиотеке университета (включая доступ к ЭБС), публичных научно-технических библиотеках. Закрепление результатов практики осуществляется путем самостоятельной работы студентов с рекомендуемой литературой.

В ходе прохождения практики студент должен решить все поставленные перед ним задачи и написать отчет о своей деятельности в рамках практики, а также выполненные работы (трудовые действия, трудовые функции), связанные с будущей профессиональной деятельностью обучающегося.. В отчете должны быть описаны все основные этапы прохождения практики в соответствии с заданием. Окончательно оформленный и

подписанный студентом отчет сдается руководителю практики не позже, чем за 3 дня до защиты. В указанное руководителем практики время студент обязан явиться на кафедру для защиты отчета.

8.6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБУЧЕНИЮ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Освоение практики обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиа материалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.