



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмова

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ ИНФОРМАЦИИ

Направление подготовки (специальность)

09.03.03 Прикладная информатика

Направленность (профиль/специализация) программы

Искусственный интеллект в цифровой экономике

Уровень высшего образования - бакалавриат

Форма обучения

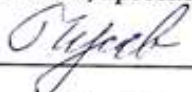
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	3
Семестр	6

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес-информатики и информационных технологий 25.01.2022, протокол № 5

Зав. кафедрой  Г.Н. Чусавитина

Рабочая программа одобрена методической комиссией ИЭиАС 26.01.2022 г. протокол № 5

Председатель  В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры БиИТ, канд. пед. наук  Е.В. Чернова

Рецензент:
Генеральный директор ООО
«Корпоративные системы Плюс»,  Ю.А. Чудинова

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.Н. Чусавитина

1 Цели освоения дисциплины (модуля)

Целью преподавания дисциплины является изучение основных концепций и практических аспектов в сфере защиты информации с использованием методов искусственного интеллекта.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Применение искусственного интеллекта в защите информации входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Программирование на Python

Интеллектуальный анализ данных

Управление данными

Машинное обучение

Разработка интеллектуальных приложений в среде 1С

Производственная - технологическая (проектно-технологическая) практика

Искусственные нейронные сети

Разработки Web-приложений на Python

Большие данные в цифровой экономике

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Выполнение и защита выпускной квалификационной работы

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Применение искусственного интеллекта в защите информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1	Способен использовать, создавать и внедрять технологии искусственного интеллекта для решения задач в зависимости от особенностей проблемной и предметной областей
ПК-1.1	Осуществляет поиск данных в открытых источниках, специализированных библиотеках, репозиториях и архивах, выполняет подготовку, разметку, анализ, представление и визуализацию больших данных
ПК-1.2	Создает, поддерживает и использует системы искусственного интеллекта, методы и модели машинного обучения для решения задач искусственного интеллекта
ПК-1.3	Осуществляет оценку и выбор моделей искусственных нейронных сетей и инструментальных средств, использует и разрабатывает системы искусственного интеллекта на основе нейросетевых моделей и методов для решения поставленной задачи

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

- контактная работа – 114,5 акад. часов;
- аудиторная – 110 акад. часов;
- внеаудиторная – 4,5 акад. часов;
- самостоятельная работа – 29,8 акад. часов;
- в форме практической подготовки – 0 акад. час;
- подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Введение в защиту информации средствами искусственного интеллекта								
1.1 Введение в защиту информации. Основные задачи. Кейсы применения методов ИИ в защите информации	8	6				Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Эссе	ПК-1.1
1.2 Проблемы информационной безопасности искусственного интеллекта		4	8			Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию	Семинар по темам: - Системы ИИ с централизованным управлением - Deepfakes - Отравление данных - Анализ тональности - Целевые атаки моделями машинного обучения - Атаки на узкие места машинного обучения	ПК-1.1

1.3	Применение искусственного интеллекта информационной безопасности	в	2	8		4	Конспектирован ие учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию	Семинар по темам: - Биометрическая идентификация личности системами ИИ - Обнаружение вторжений в компьютерные системы средствами ИИ - Выявление ботов средствами ИИ - Выявление мошенничества средствами ИИ - Оценка рисков информационной безопасности средствами ИИ - Определение утечек данных	ПК-1.1	
Итого по разделу			12	16		4				
2. Модели представления знаний для защиты информации										
2.1	Модели представления знаний для защиты информации		8	4	4		4,8	Конспектирован ие учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Представление знаний в виде правил"	
Итого по разделу			4	4		4,8				
3. Экспертные системы в защите информации										
3.1	Экспертные системы в защите информации		8	8	14		4	Конспектирован ие учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Разработка экспертной системы на языке логического программирования" Лабораторная работа "Разработка экспертной системы на основе байесовского вывода" Лабораторная работа "Разработка экспертной системы на основе нечеткого вывода"	ПК-1.1, ПК-1.2, ПК-1.3

3.2	Бионические алгоритмы оптимизации		4	4		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Бионические алгоритмы оптимизации"	ПК-1.1, ПК-1.2, ПК-1.3
Итого по разделу			12	18		8			
4. Машинное обучение для решения задач по защите информации									
4.1	Базовые алгоритмы машинного обучения в вопросах защиты информации		4	8		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Базовые алгоритмы машинного обучения. Регрессионный анализ"	ПК-1.1, ПК-1.2, ПК-1.3
4.2	Композиции алгоритмов машинного обучения для решения вопросов защиты информации	8	6	8		5	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Композиции алгоритмов машинного обучения"	ПК-1.1, ПК-1.2, ПК-1.3
4.3	Нейросетевые модели машинного обучения в защите информации		6	12		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Лабораторная работа "Однослойная нейронная сеть" Лабораторная работа "Многослойная нейронная сеть" Лабораторная работа "Распознавание образов с помощью перцептронов"	ПК-1.1, ПК-1.2, ПК-1.3
Итого по разделу			16	28		13			
Итого за семестр			44	66		29,8		экзамен	
Итого по дисциплине			44	66		29,8		экзамен	

5 Образовательные технологии

При проведении занятий и организации самостоятельной работы бакалавров используются:

Традиционные технологии обучения, предполагающие передачу информации в готовом виде, формирование учебных умений по образцу: лекция-изложение, лекция-объяснение, лабораторные работы, контрольная работа и др.

Использование традиционных технологий обеспечивает ориентирование студента в потоке информации, связанной с различными подходами к определению сущности, содержания, методов, форм развития и саморазвития личности; самоопределение в выборе оптимального пути и способов личностно-профессионального развития; систематизацию знаний, полученных студентами в процессе аудиторной и самостоятельной работы. Лабораторные занятия обеспечивают развитие и закрепление умений и навыков определения целей и задач саморазвития, а также принятия наиболее эффективных решений по их реализации.

Интерактивные формы обучения, предполагающие организацию обучения как продуктивной творческой деятельности в режиме взаимодействия студентов друг с другом и с преподавателем

Использование интерактивных образовательных технологий способствует повышению интереса и мотивации учащихся, активизации мыслительной деятельности и творческого потенциала студентов, делает более эффективным усвоение материала, позволяет индивидуализировать обучение и ввести экстренную коррекцию знаний.

При проведении лабораторных занятий используются групповая работа, технология коллективной творческой деятельности, технология сотрудничества. Данные технологии обеспечивают высокий уровень усвоения студентами знаний, эффективное и успешное овладение умениями и навыками в предметной области, формируют познавательную потребность и необходимость дальнейшего самообразования, позволяют активизировать исследовательскую деятельность, обеспечивают эффективный контроль усвоения знаний

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Чесалин, А. Н. Основы искусственного интеллекта с приложениями в информационной безопасности : учебное пособие / А. Н. Чесалин. — Москва : РТУ МИРЭА, 2021. — 155 с. — ISBN 978-5-7339-1589-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/182429> (дата обращения: 26.06.2022). — Режим доступа: для авториз. пользователей.

б) Дополнительная литература:

1. Чесалин, А. Н. Основы искусственного интеллекта с приложениями в информационной безопасности. Практикум : учебное пособие / А. Н. Чесалин. — Москва : РТУ МИРЭА, 2020. — 75 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163838> (дата обращения: 26.06.2022). — Режим доступа: для авториз. пользователей.

2. Защита информации в центрах обработки данных : учебно-методическое пособие / И. А. Ушаков, В. А. Десницкий, А.А. Чечулин, Т. Е. Захарова. —

Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. — 44 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/180094>. — Режим доступа: для авториз. пользователей

3. Мещерина, Е. В. Системы искусственного интеллекта : учебно-методическое пособие / Е. В. Мещерина. — Оренбург : ОГУ, 2019. — 96 с. — ISBN 978-5-7410-2315-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/160008> (дата обращения: 26.06.2022). — Режим доступа: для авториз. пользователей.

в) Методические указания:

Методические рекомендации по дисциплине представлены в приложении 3

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно	бессрочно
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандарт	Д-162-21 от 26.03.2021	26.03.2023
Linux Calculate	свободно	бессрочно
FAR Manager	свободно	бессрочно
Браузер Yandex	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяе	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И.	https://magtu.informsystema.ru/Marc.html?locale=ru
Университетская информационная система	https://uisrussia.msu.ru
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения занятий лекционного типа: специализированная (учебная) мебель (столы, стулья, доска аудиторная), мультимедийное оборудование (проектор, компьютер, экран) для презентации учебного материала по дисциплине;

Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки): специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Помещение для хранения и профилактического обслуживания учебного оборудования: мебель (столы, стулья, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации), персональные компьютеры

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Применение искусственного интеллекта в защите информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа бакалавров.

Аудиторная самостоятельная работа бакалавров предполагает решение и оформление согласно заданным требованиям заданий лабораторных работ. Требования к оформлению находятся в СМК-О-СМГТУ-42-09 Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения учебной и научной литературы по соответствующему разделу с проработкой материала, участие в дистанционном курсе или изучении MOOK, предложенном преподавателем и выполнения домашних заданий (подготовка к лабораторным работам) с консультациями преподавателя.

Оценочные средства для проведения промежуточной аттестации
а) Планируемые результаты обучения и оценочные средства для проведения
промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-1 – Способен использовать, создавать и внедрять технологии искусственного интеллекта для решения задач в зависимости от особенностей проблемной и предметной областей		
ПК-1.1	Осуществляет поиск данных в открытых источниках, специализированных библиотеках, репозиториях и архивах, выполняет подготовку, разметку, анализ, представление и визуализацию больших данных	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> 1. Стандарты безопасности информационных технологий. 1. Классификация систем искусственного интеллекта для защиты информации 2. Этическая сторона применения ИИ в защите информации 3. Продукционная модель представления знаний в безопасности. 4. Проблемы защиты информации в развитии систем искусственного интеллекта
ПК-1.2	Создает, поддерживает и использует системы искусственного интеллекта, методы и модели машинного обучения для решения задач искусственного интеллекта	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> 1. Экспертные системы в обеспечении защиты информации <p>Практическое задание</p> <p>Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач:</p> <ul style="list-style-type: none"> - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте - выбор подходящего решения для обеспечения безопасности корпоративной сети
ПК-1.3	Осуществляет оценку и выбор моделей искусственных нейронных сетей и инструментальных средств, использует и разрабатывает системы искусственного интеллекта на основе нейросетевых моделей и методов для решения поставленной задачи	<p>Перечень теоретических вопросов</p> <ol style="list-style-type: none"> 1. Базовые алгоритмы машинного обучения в информационной безопасности. 2. Применение алгоритма Random Forest для защиты информации. 3. Применение алгоритма AdaBoost для защиты информации. 4. Нейросетевые алгоритмы машинного обучения в защите информации 5. Базовые алгоритмы машинного обучения в информационной безопасности. <p>Практическое задание</p> <p>Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач:</p> <ul style="list-style-type: none"> - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		- выбор подходящего решения для обеспечения безопасности корпоративной сети

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Применение искусственного интеллекта в защите информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета с оценкой.

Зачет по данной дисциплине проводится в устной форме по зачетным билетам, каждый из которых включает один теоретический вопрос и одно практическое задание.

Показатели и критерии оценивания зачета с оценкой:

«Отлично» – оценка знаний студента, который свободно владеет:

- 1) понятийно-терминологической базой дисциплины и знает значение наиболее часто используемых аббревиатур;
- 2) четко увязывает теоретическое познание дисциплины с реальной практикой;
- 3) знаком с широким кругом литературных источников, знает, где их достать, хорошо разбирается в истории становления дисциплины, в оценке ее текущего состояния и перспектив ее развития;
- 4) полностью владеет материалом практического задания, четко и аргументировано защищает ее положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

«Хорошо» – оценка знаний студента, который владеет понятийно-терминологической базой дисциплины, может увязать теоретическое познание дисциплины с реальной практикой. Владеет материалом практической работы, показал способность к объяснению смысла основных положений;

«Удовлетворительно» – оценка знаний студента, который в большей части владеет, с небольшими изъянами, понятийно-терминологической базой дисциплины, имеет представление о внутренней логике дисциплины, представленной в виде учебной программы, Владеет, но неуверенно, материалом практического задания.

«Неудовлетворительно» – оценка знаний студента, который не владеет понятийно-терминологической базой дисциплины и материалом практического задания.

Методические рекомендации для студентов ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Осваивая курс, бакалавру необходимо научиться работать на лекциях, на лабораторных занятиях и организовывать самостоятельную внеаудиторную деятельность.

В начале лекции необходимо уяснить цель, которую лектор ставит перед собой и студентами. Важно внимательно слушать лектора, отмечать наиболее существенную информацию и кратко записывать ее в тетрадь. Сравнить то, что услышано на лекции с прочитанным и усвоенным ранее, укладывать новую информацию в собственную, уже имеющуюся, систему знаний.

По ходу лекции важно подчеркивать новые термины, устанавливая их взаимосвязь с понятиями, научиться использовать новые понятия в учебной деятельности.

Необходимо очень тщательно вслед за лектором делать рисунки, графики, схемы. Если лектор приглашает к дискуссии, необходимо принять в ней участие.

Если на лекции бакалавр не получил ответа на возникшие у него вопросы, необходимо в конце лекции задать их лектору. Дома необходимо прочитать записанную лекцию, подчеркнуть наиболее важные моменты, составить словарь новых терминов.

Зная тему практического занятия, необходимо готовиться к нему заблаговременно. Для этого необходимо изучить лекционный материал, соответствующий теме занятия и рекомендованный преподавателем материал из учебной литературы.

В процессе подготовки к занятиям необходимо воспользоваться материалами учебно-методического комплекса дисциплины, материалами, рекомендованными преподавателем и самостоятельно найденными материалами.

Важнейшей особенностью обучения в высшей школе является высокий уровень самостоятельности студентов в ходе образовательного процесса. Эффективность самостоятельной работы зависит от таких факторов как:

- уровень мотивации бакалавров к овладению конкретными знаниями и умениями;
- наличие навыка самостоятельной работы, сформированного на предыдущих этапах обучения;
- наличие четких ориентиров самостоятельной работы.

Приступая к самостоятельной работе, необходимо получить следующую информацию:

- цель изучения конкретного учебного материала;
- место изучаемого материала в системе знаний, необходимых для формирования специалиста;
- перечень знаний и умений, которыми должен овладеть студент;
- порядок изучения учебного материала;
- источники информации;
- форма и способ фиксации результатов выполнения учебных заданий;
- сроки выполнения самостоятельной работы.

Эта информация представлена в учебно-методическом комплексе дисциплины на портале.

При выполнении самостоятельной работы рекомендуется:

- записывать ключевые слова и основные термины,
- составлять словарь основных понятий,
- составлять таблицы, схемы, графики и т.д.
- писать краткие рефераты по изучаемой теме.

Следует выполнять рекомендуемые упражнения и задания.

Результатом самостоятельной работы должна быть систематизация и структурирование учебного материала по изучаемой теме, включение его в уже имеющуюся у студента систему знаний.

После изучения учебного материала необходимо проверить усвоение учебного материала с помощью предлагаемых контрольных вопросов и при необходимости повторить учебный материал.

В процессе подготовки к зачету необходимо систематизировать, запомнить учебный материал, научиться применять его на практике.

Основными способами приобретения знаний, как известно, являются: чтение учебника и дополнительной литературы, рассказ и объяснение преподавателя, поиск ответа на контрольные вопросы.

Приобретение новых знаний требует от учащегося определенных усилий и активной работы на каждом этапе формирования знаний. Знания, приобретенные учащимся в ходе активной самостоятельной работы, являются более глубокими и прочными.

Изучая данную дисциплину, бакалавр сталкивается с необходимостью понять и запомнить большой по объему учебный материал. Запомнить его очень важно, так как даже интеллектуальные и операционные умения и навыки для своей реализации требуют определенных теоретических знаний.

Важнейшим условием для успешного формирования прочных знаний является их упорядочивание, приведение их в единую систему. Это осуществляется в ходе выполнения учащимся следующих видов работ по самостоятельному структурированию учебного материала:

- запись ключевых терминов,
- составление словаря терминов,
- составление словаря ГОСТов,
- составление таблиц,
- составление схем,
- составление классификаций,
- выявление причинно-следственных связей,
- составление опорных схем и конспектов.

Информация, организованная в систему, где учебные элементы связаны друг с другом различного рода связями (функциональными, логическими и др.), лучше запоминается.