МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭнАС
В.Р. Храмшин

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЗАЩИТА ИНФОРМАЦИИ МЕТОДАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Направление подготовки (специальность)
09.04.03 Прикладная информатика

Направленность (профиль/специализация) программы
Технологии Data Science

Уровень высшего образования - магистратура

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	2
Семестр	3

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916)

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 БИиИТ, 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

1 Цели освоения дисциплины (модуля)

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

Задачами изучения дисциплины являются:

1. Ознакомить с основными задачами защиты информации, кейсами применения методов ИИ в защите информации.

2. Познакомить студентов с определением, классификацией и характеристиками сетевых атак и способов защиты, способами анализа сетевого трафика методами ИИ.

3. Рассмотреть основные технологические принципы устройства антивирусов, анализа вредоносной активности методами ИИ.

4. Разобрать на практике методы и способы противодействия мошенничеству, реализации антиспам-фильтров и антифрод-систем

2 Место дисциплины (модуля) в структуре образовательной программы

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

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

Библиотеки языка программирования Python для Data Science

Инженирия знаний и экспертные системы

Производственная - технологическая (проектно-технологическая) практика

Базы данных и знаний

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

Выполнение и защита выпускной квалификационной работы

Производственная - научно-исследовательский семинар "Технологии Data Science"

Производственная-преддипломная практика

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

В результате освоения дисциплины (модуля) «Защита информации методами искусственного интеллекта» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-2 Способен применять современные методы и инструментальные средства Data Science для автома-тизации и информа-тизации решения прикладных задач различных классов	
ПК-2.1	Осуществляет выбор и применение методов инженерии знаний для создания систем, основанных на знаниях
ПК-2.2	Осуществляет создание, поддержку и использование систем бизнес-аналитики в организации
ПК-2.3	Осуществляет подготовку и интеллектуальную обработку данных, разрабатывает и применяет методы и алгоритмы машинного обучения
ПК-2.4	Осуществляет создание, поддержку и использование нейросетевых моделей и методов для решения поставленной задачи
ПК-2.5	Осуществляет аналитические работы, участвует в проектах создания и развития систем с использованием технологий больших данных

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 37 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 1 акад. часов;

– самостоятельная работа – 71 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

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								
1.1 Введение в защиту информации. Основные задачи. Кейсы применения методов ИИ в защите информации	3	4	2		6	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию	Семинар по кейсам применения методов ИИ в защите информации	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
Итого по разделу		4	2		6			
2. Сетевые атаки и способы защиты. Анализ сетевого трафика методами ИИ								
2.1 Сетевые атаки и способы защиты	3	4	4		16	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Практические занятия по анализу сетевого трафика методами ИИ.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
2.2 Анализ сетевого трафика методами ИИ		4	4		16	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Выявление аномалий по признаковому описанию трафика. Профилизация трафика на основе методов машинного обучения.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
Итого по разделу		8	8		32			
3. Типы вредоносной активности. Антивирусы. Анализ вредоносной активности методами ИИ								

3.1 Типы вредоносной активности. Антивирусы. Анализ вредоносной активности методами ИИ	3	2	4		20	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию	Семинар по кейсам выявления вредоносной активности методами ИИ	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
Итого по разделу		2	4		20			
4. Противодействие мошенничеству. Антиспам. Анализ контента на примере почтовых сервисов								
4.1 Противодействие мошенничеству. Антиспам.	3	2	2		8	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Практические занятия по выявлению спама в почтовых сервисах	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
4.2 Анализ контента на примере почтовых сервисов		2	2		5	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Реализация спам-фильтров методами интеллектуального анализа текста	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4, ПК-2.5
Итого по разделу		4	4		13			
Итого за семестр		18	18		71		зао	
Итого по дисциплине		18	18		71		зачет с оценкой	

5 Образовательные технологии

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Практическая работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

В ходе проведения всех практических занятий предусматривается использование средств вычислительной техники при выполнении индивидуальных заданий и контрольной работы. Текущий, промежуточный и рубежный контроль проводится с помощью образовательного портала

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

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 распространяемое ПО	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

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Защита информации методами искусственного интеллекта» предусмотрена самостоятельная работа магистрантов.

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

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

Вопросы для самостоятельного изучения:

Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач:

- определение стойкости парольной фразы
- оценка надежности телекоммуникационной сети
- определение спама в электронной почте
- выбор подходящего решения для обеспечения безопасности корпоративной сети

Приложение 2

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-2 – способен применять современные методы и инструментальные средства Data Science для автоматизации и информатизации решения прикладных задач различных классов		
ПК-2.1	Осуществляет выбор и применение методов инженерии знаний для создания систем, основанных на знаниях	Перечень теоретических вопросов 1. Стандарты безопасности информационных технологий. 1. Аспекты безопасности информации. 2. Основные виды угроз. 3. Цели и функции защиты информации. 4. Защита информации от случайных угроз 5. Классификация систем искусственного интеллекта для защиты информации 6. Этическая сторона применения ИИ в защите информации 7. Продукционная модель представления знаний в безопасности.
ПК-2.2	Осуществляет создание, поддержку и использование систем бизнес-аналитики в организации	Перечень теоретических вопросов 1. Экспертные системы в обеспечении защиты информации Практическое задание Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач: - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте - выбор подходящего решения для обеспечения безопасности корпоративной сети
ПК-2.3	Осуществляет подготовку и интеллектуальную обработку данных, разрабатывает и применяет методы и алгоритмы машинного обучения	Перечень теоретических вопросов 1. Базовые алгоритмы машинного обучения в информационной безопасности. 2. Применение алгоритма Random Forest для защиты информации. 3. Применение алгоритма AdaBoost для защиты информации. Практическое задание Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач: - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте - выбор подходящего решения для обеспечения безопасности корпоративной сети
ПК 2.4	Осуществляет создание,	Перечень теоретических вопросов

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	поддержку и использование нейросетевых моделей и методов для решения поставленной задачи	1. Нейросетевые алгоритмы машинного обучения в защите информации 2. Базовые алгоритмы машинного обучения в информационной безопасности. Практическое задание Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач: - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте - выбор подходящего решения для обеспечения безопасности корпоративной сети
ПК 2.5	Осуществляет аналитические работы, участвует в проектах создания и развития систем с использованием технологий больших данных	Перечень теоретических вопросов 1. Проблемы защиты информации в развитии систем искусственного интеллекта Практическое задание Разработать экспертную систему на основе нечеткого логического вывода используя библиотеку scikit-fuzzy для одной из следующих задач: - определение стойкости парольной фразы - оценка надежности телекоммуникационной сети - определение спама в электронной почте - выбор подходящего решения для обеспечения безопасности корпоративной сети

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

Промежуточная аттестация по дисциплине «Защита информации методами искусственного интеллекта» 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.

Приложение 3

Методические рекомендации для студентов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Осваивая курс, магистранту необходимо научиться организовывать самостоятельную внеаудиторную деятельность.

По ходу изучения теоретического материала важно подчеркивать новые термины, устанавливать их взаимосвязь с понятиями, научиться использовать новые понятия в учебной деятельности. Необходимо очень тщательно делать рисунки, графики, схемы, подчеркнуть наиболее важные моменты, составить словарь новых терминов.

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 магистрантов 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, магистрант 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.

В качестве контрольных точек по дисциплине предусмотрена защита 10 практических работ на протяжении всего семестра, выполнение прикладного исследования и тест по теоретическому материалу, а также сдача зачета с оценкой в конце семестра. Все практические работы выполняются в предметной области магистерского исследования, либо для организации, предложенной преподавателем.