Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет физико-математических и естественных наук
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

38.03.05 БИЗНЕС-ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

КИБЕРБЕЗОПАСНОСТЬ В ЭКОНОМИКЕ
(наименование (профиль/специализация) ОП ВО)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Искусственный интеллект и кибербезопасность» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 5 разделов и 10 тем и направлена на изучение прикладных задач кибербезопасности и базовых методов искусственного интеллекта и их особенностей.

Целью освоения дисциплины является ознакомление с прикладными задачами кибербезопасности, решаемыми методами искусственного интеллекта, и изучение принципов безопасности самих методов искусственного интеллекта.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Искусственный интеллект и кибербезопасность» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	**Компетенция**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
ПК-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	ПК-4.1 Знает языки визуального моделирования; ПК-4.2 Умеет анализировать и оценивать факторы и условия, влияющие на принятие управленческих решений; ПК-4.3 Умеет проводить оценку эффективности принятия решения в соответствии с выбранными критериями или выбранными целевыми показателями;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	ПК-5.1 Знает методы организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.2 Знает основы нормативно-правового регулирования в РФ и иных странах в области защиты информации; ПК-5.3 Умеет применять методы управления кибербезопасностью предприятий и иных экономических систем; ПК-5.4 Умеет использовать нормативно-правовую базу РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем; ПК-5.5 Владеет навыкками организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.6 Владеет навыками применения нормативно-правовой базы РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Искусственный интеллект и кибербезопасность» относится к блоку по выбору блока образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Искусственный интеллект и кибербезопасность».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ПК-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	Микроэкономика и менеджмент; Макроэкономика; Архитектура предприятия; ИТ-инфраструктура предприятия; Моделирование бизнес-процессов; Технологии обеспечения кибербезопасности предприятий; Защита сетей и кибербезопасность; Киберполигон;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	Экономическая безопасность; Цифровая трансформация глобальной экономики; Киберполитика в международных экономических отношениях; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве; Защита сетей и кибербезопасность; Анализ и показатели эффективности кибербезопасности предприятия; Имитационное моделирование угроз экономической кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования; Киберполигон; Кибербезопасность платежных систем;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Искусственный интеллект и кибербезопасность» составляет «4» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			7
Контактная работа, ак.ч.	*72*		*72*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	36		36
Самостоятельная работа обучающихся, ак.ч.	*45*		*45*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	О задачах кибербезопасности, связанных с развитием искусственного интеллекта	1.1	Ознакомление с кругом задач кибербезопасности, решаемых методами искусственного интеллекта	ЛК, СЗ
		1.2	Прикладные задачи кибербезопасности, связанные с определением авторства текста	ЛК, СЗ
Раздел 2	Методы идентификации авторства текста	2.1	Признаки текста, использующиеся для идентификации автора	ЛК, СЗ
		2.2	Подходы к решению задачи идентификации	ЛК, СЗ
Раздел 3	Большие языковые модели, обработка текста и кибербезопасность	3.1	Языковые модели	ЛК, СЗ
		3.2	Модели LLM (GPT-3, ChatGPT, GPT-4) в задачах обработки текстов	ЛК, СЗ
Раздел 4	Безопасность систем искусственного интеллекта	4.1	Атаки на системы машинного обучения	ЛК, СЗ
		4.2	Анализ и предотвращение угроз	ЛК, СЗ
Раздел 5	Методы интерпретации моделей машинного обучения	5.1	Методы «локального» объяснения	ЛК, СЗ
		5.2	Методы «глобального» объяснения	ЛК, СЗ

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.*

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.Дополнительное ПО: офисный пакет MS Office или LibreOffice.

Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.Дополнительное ПО: офисный пакет MS Office или LibreOffice.

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Мельников Сергей Юрьевич. Искусственный интеллект и кибербезопасность : учебное пособие / С.Ю. Мельников. - Электронные текстовые данные. - Москва : РУДН, 2023. - 72 с. : ил.
URL: https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515838&idb=0

2. Платонов, А. В. Машинное обучение : учебное пособие для вузов / А. В. Платонов. — Москва : Издательство Юрайт, 2022. — 85 с. — (Высшее образование). — ISBN 978-5-534-15561-7. — Текст : электронный // Образовательная платформа Юрайт [сайт].

3. Воронцов К. В. Математические методы обучения по прецедентам. Курс лекций. [Электронный ресурс] / Режим доступа: http://www.machinelearning.ru/wiki/images/6/6d/voron-ml-1.pdf, свободный (дата обращения 24.04.2022).

4. Захаров В. П., Богданова С. Ю. Корпусная лингвистика. Учебник. 3-е издание, переработанное. Издательство СПбГУ, 2020.

Дополнительная литература:

1. Грас Д. Data Science. Наука о данных с нуля: Пер. с англ.- 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2021. – 416с.: ил.

2. Васильев А.Н. Python на примерах. Практический курс по программированию. – СПб.: Наука и техника, 2016. – 432с.: ил.

3. Федоров, Д. Ю. Программирование на языке высокого уровня Python : учебное пособие для прикладного бакалавриата/ Д. Ю. Федоров. — М.: Издательство Юрайт, 2017. — 126 с.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН http://lib.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС Юрайт http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Искусственный интеллект и кибербезопасность».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Искусственный интеллект и кибербезопасность» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Мельников Сергей Юрьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*