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

**Факультет искусственного интеллекта**

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

**Рекомендована МССН для направления подготовки/специальности:**

**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

(код и наименование направления подготовки/специальности)

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

**ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)**

(наименование (профиль/специализация) ОП ВО)

**2025 г.**

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Технологии искусственного интеллекта в задачах кибербезопасности» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 5 разделов и 10 тем и направлена на изучение прикладных задач информационной безопасности и базовых методов искусственного интеллекта, их особенностей.

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

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Технологии искусственного интеллекта в задачах кибербезопасности» 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) |
|---|---|---|
| ОПК-1 | Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | ОПК-1.1 Оценивает роль информации, информационных технологий и информационной безопасности в современном обществе;<br>ОПК-1.2 Оценивает значение информации, информационных технологий и информационной безопасности для обеспечения объективных потребностей личности, общества и государства; |
| ОПК-2 | Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности | ОПК-2.1 Применяет информационно-коммуникационные технологии для решения задач профессиональной деятельности;<br>ОПК-2.2 Применяет программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; |

## 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Технологии искусственного интеллекта в задачах кибербезопасности» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Технологии искусственного интеллекта в задачах кибербезопасности».

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

| **Шифр** | **Наименование компетенции** | **Предшествующие дисциплины/модули, практики*** | **Последующие дисциплины/модули, практики*** |
|---|---|---|---|
| ОПК-1 | Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства | Информатика;<br>Основы информационной безопасности (введение в специальность);<br>Информационные технологии;<br>Операционные системы;<br>Сети и системы передачи информации; | Базы данных, системы управления базами данных;<br>Эксплуатационная практика;<br>Технологическая практика; |
| ОПК-2 | Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности | Информационные технологии;<br>Операционные системы;<br>Сети и системы передачи информации;<br>Языки программирования;<br>Технологии и методы программирования; | Эксплуатационная практика;<br>Технологическая практика;<br>Исследовательская практика;<br>Базы данных, системы управления базами данных;<br>Программно-аппаратные средства защиты информации; |

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

** - элективные дисциплины /практики

## 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Технологии искусственного интеллекта в задачах кибербезопасности» составляет «3» 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)** |
|---|---|---|---|
| | | | **4** |
| *Контактная работа, ак.ч.* | *68* | | *68* |
| Лекции (**ЛК**) | 34 | | 34 |
| Лабораторные работы (**ЛР**) | 0 | | 0 |
| Практические/семинарские занятия (**СЗ**) | 34 | | 34 |
| *Самостоятельная работа обучающихся, ак.ч.* | *22* | | *22* |
| *Контроль (экзамен/зачет с оценкой), ак.ч.* | *18* | | *18* |
| **Общая трудоемкость дисциплины** | **ак.ч.** | ***108*** | *108* |
| | **зач.ед.** | ***3*** | *3* |

## 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.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.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, GNU Octave, Scilab. |

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

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

*Основная литература:*

1. 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].

2. 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).

3. 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 «Технологии искусственного интеллекта в задачах кибербезопасности».

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

**РАЗРАБОТЧИК:**

| Доцент кафедры прикладной информатики и теории вероятностей | | Мельников Сергей Юрьевич |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ БУП:**

| Заведующий кафедрой | | Подолько Павел Михайлович [М\|] заведующий кафедрой |
|---|---|---|
| *Должность БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ ОП ВО:**

| Заведующий кафедрой прикладной информатики и теории вероятностей | | Самуйлов Константин Евгеньевич |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |