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

Институт русского языка
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КИБЕРБЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

45.03.04 ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ В ГУМАНИТАРНОЙ СФЕРЕ
(код и наименование направления подготовки/специальности)

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

КИБЕРТЕХНОЛОГИИ И АНАЛИЗ ДАННЫХ В ГУМАНИТАРНОЙ СФЕРЕ
(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Кибербезопасность интеллектуальных систем» входит в программу бакалавриата «Кибертехнологии и анализ данных в гуманитарной сфере» по направлению 45.03.04 «Интеллектуальные системы в гуманитарной сфере» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра прикладной информатики и интеллектуальных систем в гуманитарной сфере. Дисциплина состоит из 5 разделов и 11 тем и направлена на изучение способов и подходов к обеспечению информационной безопасности интеллектуальных систем, а также программных средств, используемых для обеспечения защиты информации в интеллектуальных системах.

Целью освоения дисциплины является приобретение обучающимися знаний и навыков о методах и средствах защиты информации, обрабатываемой в системах искусственного интеллекта.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Кибербезопасность интеллектуальных систем» 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)
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	УК-12.3 Проводит оценку информации и её достоверности;
ПК-4	Способен выявлять требования к интеллектуальным системам в гуманитарной сфере и проектным решениям в гуманитарной сфере	ПК-4.2 Вырабатывает предложения по проектным решениям в гуманитарной предметной области; ПК-4.3 Выявляет исходные требования к проектируемым интеллектуальным системам на основе анализа гуманитарной предметной области;
ПК-5	Способен выполнять обследование текущей ситуации и анализ проблем, требующих автоматизированного решения, в гуманитарной предметной области	ПК-5.5 Управляет исследованием текущей ситуации и анализом проблем, требующих автоматизированного решения, в гуманитарной предметной области;
ПК-6	Способен осуществлять концептуально-логическое проектирование	ПК-6.1 Формулирует исходные требования к концепции проектируемых интеллектуальных систем в гуманитарной сфере;

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	интеллектуальных систем в гуманитарной сфере	

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Кибербезопасность интеллектуальных систем» относится к части, формируемой участниками образовательных отношений 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 «Кибербезопасность интеллектуальных систем».

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
УК-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	История России; Математическое обеспечение кибертехнологий в гуманитарной сфере; Аналитико-алгоритмическое обеспечение кибертехнологий в гуманитарной сфере; Информационное обеспечение кибертехнологий в гуманитарной сфере; Программное обеспечение кибертехнологий в гуманитарной сфере; Интеллектуальные кибертехнологии в гуманитарной сфере; *Иностранный язык***; *Русский язык как иностранный***; Введение в языкознание; Введение в социологию; Теория перевода; Морфология и синтаксис; Введение в семиотику; Базовый курс литературоведения; Введение в корпусную лингвистику; *Методы исследований в лингвистике и переводе***; *Методы исследований в социологии***; *Методы исследований в истории и литературе***; *Кибертехнологии в лингвистике и переводе***; *Кибертехнологии в социологии***; *Кибертехнологии в истории и литературе***;	Интеллектуальные кибертехнологии в гуманитарной сфере; Архитектурное проектирование интеллектуальных кибертехнологий в гуманитарной сфере; *Русский язык как иностранный в профессиональных целях***; *Иностранный язык (основной) в профессиональных целях***; *Прикладные аспекты применения кибертехнологий в лингвистике и переводе***; *Прикладные аспекты применения кибертехнологий в социологии***; *Прикладные аспекты применения кибертехнологий в истории и литературе***; Разработка проектной документации: практический курс; Преддипломная практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		Ознакомительная практика; Технологическая практика (учебная); Проектно-технологическая практика;	
ПК-6	Способен осуществлять концептуально-логическое проектирование интеллектуальных систем в гуманитарной сфере	Аналитико-алгоритмическое обеспечение кибертехнологий в гуманитарной сфере; Программное обеспечение кибертехнологий в гуманитарной сфере; Интеллектуальные кибертехнологии в гуманитарной сфере; Математическое обеспечение кибертехнологий в гуманитарной сфере; Технологическая практика (учебная); Проектно-технологическая практика;	Интеллектуальные кибертехнологии в гуманитарной сфере; Архитектура программного обеспечения; Архитектурное проектирование интеллектуальных кибертехнологий в гуманитарной сфере; Управление полным жизненным циклом интеллектуальных кибертехнологий в гуманитарной сфере; *Прикладные аспекты применения кибертехнологий в лингвистике и переводе***; *Прикладные аспекты применения кибертехнологий в социологии***; *Прикладные аспекты применения кибертехнологий в истории и литературе***; Преддипломная практика;
ПК-4	Способен выявлять требования к интеллектуальным системам в гуманитарной сфере и проектным решениям в гуманитарной сфере	*Кибертехнологии в лингвистике и переводе***; *Кибертехнологии в социологии***; Аналитико-алгоритмическое обеспечение кибертехнологий в гуманитарной сфере; Программное обеспечение кибертехнологий в гуманитарной сфере; Интеллектуальные кибертехнологии в гуманитарной сфере; *Кибертехнологии в истории и литературе***; *Методы исследований в лингвистике и переводе***; *Методы исследований в социологии***; *Методы исследований в истории и литературе***; Математическое обеспечение кибертехнологий в гуманитарной сфере; Ознакомительная практика; Технологическая практика	Преддипломная практика; Интеллектуальные кибертехнологии в гуманитарной сфере; Управление полным жизненным циклом интеллектуальных кибертехнологий в гуманитарной сфере; *Прикладные аспекты применения кибертехнологий в лингвистике и переводе***; *Прикладные аспекты применения кибертехнологий в социологии***; *Прикладные аспекты применения кибертехнологий в истории и литературе***; Архитектура программного обеспечения; Архитектурное проектирование

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		(учебная); Проектно-технологическая практика;	интеллектуальных кибертехнологий в гуманитарной сфере;
ПК-5	Способен выполнять обследование текущей ситуации и анализ проблем, требующих автоматизированного решения, в гуманитарной предметной области	*Кибертехнологии в лингвистике и переводе**; Кибертехнологии в социологии**; Аналитико-алгоритмическое обеспечение кибертехнологий в гуманитарной сфере; Программное обеспечение кибертехнологий в гуманитарной сфере; Интеллектуальные кибертехнологии в гуманитарной сфере; Кибертехнологии в истории и литературе**; Методы исследований в лингвистике и переводе**; Методы исследований в социологии**; Методы исследований в истории и литературе**; Математическое обеспечение кибертехнологий в гуманитарной сфере; Информационное обеспечение кибертехнологий в гуманитарной сфере; Ознакомительная практика; Технологическая практика (учебная); Проектно-технологическая практика;	Интеллектуальные кибертехнологии в гуманитарной сфере; Архитектура программного обеспечения; Архитектурное проектирование интеллектуальных кибертехнологий в гуманитарной сфере; Управление полным жизненным циклом интеллектуальных кибертехнологий в гуманитарной сфере; *Прикладные аспекты применения кибертехнологий в лингвистике и переводе***; *Прикладные аспекты применения кибертехнологий в социологии***; *Прикладные аспекты применения кибертехнологий в истории и литературе***; 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 «Кибербезопасность интеллектуальных систем» составляет «2» зачетные единицы.

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

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			7
Контактная работа, ак.ч.	*30*		*30*
Лекции (**ЛК**)	15		15
Лабораторные работы (**ЛР**)	15		15
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*33*		*33*
Контроль (экзамен/зачет с оценкой), ак.ч.	*9*		*9*
Общая трудоемкость дисциплины	**ак.ч.**	***72***	*72*
	зач.ед.	***2***	*2*

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	Основные понятия в области информационной безопасности.	1.1	Угрозы, уязвимости, атаки, инциденты. Моделирование угроз. Модель нарушителя.	ЛК, ЛР
		1.2	Меры и основные принципы обеспечения безопасности информационных технологий.	ЛК, ЛР
Раздел 2	Введение в тему атак на интеллектуальные системы.	2.1	Методологические основы комплексной системы защиты информации систем искусственного интеллекта. Определение состава защищаемой информации.	ЛК, ЛР
		2.2	Источники, способы и результаты дестабилизирующего воздействия на информацию. Каналы и методы несанкционированного доступа к информации.	ЛК, ЛР
Раздел 3	Интеллектуальные системы как объект защиты.	3.1	Архитектура распределённых приложений. Модель «клиент-сервер», двухзвенные, трёхзвенные архитектуры. Web-приложения. Уровни информационной инфраструктуры.	ЛК, ЛР
		3.2	Жизненный цикл интеллектуальных систем.	ЛК, ЛР
		3.3	Базы знаний интеллектуальных систем.	ЛК, ЛР
Раздел 4	Основные виды атак на интеллеутальные системы.	4.1	Атаки на сетевые и серверную инфраструктуру интеллектуальных систем. DoS и DDoS-атаки. Brute-force атаки. Фишинг. Использование вредоносного ПО. Атаки «нулевого дня».	ЛК, ЛР
		4.2	Атаки на базы знаний интеллектуальных систем. Атаки отравлением. Атаки уклонением. Атаки извлечением. Атаки с применением порождающих алгоритмов.	ЛК, ЛР
Раздел 5	Основные способы защиты интеллектуальных систем.	5.1	Мониторинг событий безопасности. SIEM-системы. Защита от несанкционированного доступа. WAF-комплексы, межсетевые экраны, антивирусное ПО, системы обнаружения и предотвращения вторжений, системы предотвращения утечки данных. Шифрование данных.	ЛК, ЛР
		5.2	Основные способы защиты от атак на базы знаний интеллектуальных систем. Обфускация данных. Валидация данных. Защита исходного кода моделей. Мониторинг модели в процессе обучения.	ЛК, ЛР

* - 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.	
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 15 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	
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.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Грушо, А. А. Кибербезопасность предприятия : учебное пособие / А.А. Грушо, Е.Е. Тимонина. – Электронные текстовые данные . – Москва : РУДН, 2023. – 78 с. : ил. URL: https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=510195&idb=0.

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 (дата обращения: 24.03.2025).

3. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для вузов / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 164 с. — (Высшее образование). — ISBN 978-5-534-08687-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/514252 (дата обращения: 24.03.2025).

Дополнительная литература:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435 (дата обращения: 24.03.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300 (дата обращения: 24.03.2025).

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 https://mega.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 «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы
   - Sage https://journals.sagepub.com/
   - Springer Nature Link https://link.springer.com/
   - Wiley Journal Database https://onlinelibrary.wiley.com/
   - Наукометрическая база данных Lens.org https://www.lens.org

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

1. Курс лекций по дисциплине «Кибербезопасность интеллектуальных систем».

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

РАЗРАБОТЧИК:

Заведующий кафедрой		Софронова Елена Анатольевна
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Софронова Елена Анатольевна
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Доцент		Страшнов Станислав Викторович
Должность, БУП	*Подпись*	*Фамилия И.О.*