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

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

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

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И АНАЛИЗ ДАННЫХ
(наименование (профиль/специализация) ОП ВО)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Математические основы защиты информации и информационной безопасности» входит в программу магистратуры «Искусственный интеллект и анализ данных» по направлению 09.04.03 «Прикладная информатика» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 3 разделов и 8 тем и направлена на изучение математического аппарата современной криптографии и информационной безопасности.

Целью освоения дисциплины является овладение математическим аппаратом современной криптографии и информационной безопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Математические основы защиты информации и информационной безопасности» 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-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Знает принципы сбора, отбора и обобщения информации; УК-1.2 Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности; УК-1.3 Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов;
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы; УК-2.2 Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности; УК-2.3 Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности;
ОПК-1	Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	ОПК-1.1 Обладает фундаментальными знаниями в области математических и естественных наук, информатики и теории коммуникаций; ОПК-1.2 Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические и информационные объекты; ОПК-1.3 Имеет практический опыт работы с решением математических и информационных задач и применяет его в профессиональной деятельности;
ОПК-2	Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Знает основные положения и концепции в области программирования, языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включенного в Единый Реестр Российских программ; ОПК-2.2 Умеет анализировать типовые языки программирования, составлять программы;
ПК-2	Организационное и технологическое обеспечение	ПК-2.3 Знает основы программирования, современные методики тестирования разрабатываемых информационных

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	проектирования и дизайна ИС	систем, современные инструменты и методы верификации программного кода, теорию баз данных, системы хранения и анализа данных, инструменты и методы проектирования баз данных;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Математические основы защиты информации и информационной безопасности» 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 «Математические основы защиты информации и информационной безопасности».

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-2	Способен управлять проектом на всех этапах его жизненного цикла	Введение в компьютерные науки и искусственный интеллект; Языки программирования для задач искусственного интеллекта; Интеллектуальные системы и их применение;	Технологическая (проектно-технологическая) практика;
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Моделирование беспроводных сетей; Методы машинного обучения; Введение в компьютерные науки и искусственный интеллект; Распознавание образов и обработка изображений; Математическая теория телетрафика; Построение и анализ моделей беспроводных сетей 5G; Прикладные методы компьютерной лингвистики; Глубокое обучение и обучение с подкреплением; Показатели эффективности беспроводных сетей 5G; Модели мультисервисных сетей; Нотации моделирования и анализ бизнес-процессов; Интеллектуальные системы и их применение; Основы компьютерной лингвистики; Объектные и распределенные базы данных; Информационные базы данных;	Технологическая (проектно-технологическая) практика; Преддипломная практика;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-1	Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Ознакомительная практика; Моделирование беспроводных сетей; Методы машинного обучения; Введение в компьютерные науки и искусственный интеллект; Математическая теория телетрафика;	Технологическая (проектно-технологическая) практика;
ОПК-2	Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	Ознакомительная практика; Распознавание образов и обработка изображений; Моделирование беспроводных сетей;	Технологическая (проектно-технологическая) практика;
ПК-2	Организационное и технологическое обеспечение проектирования и дизайна ИС	Ознакомительная практика; Введение в компьютерные науки и искусственный интеллект; Распознавание образов и обработка изображений; Языки программирования для задач искусственного интеллекта; Прикладные методы компьютерной лингвистики; Глубокое обучение и обучение с подкреплением; Локальная организация интеллектуальных систем; Интеллектуальные системы и их применение; Основы компьютерной лингвистики; Показатели эффективности беспроводных сетей 5G; Построение и анализ моделей беспроводных сетей 5G; Объектные и распределенные базы данных; Нотации моделирования и анализ бизнес-процессов;	Технологическая (проектно-технологическая) практика;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО
** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Математические основы защиты информации и информационной безопасности» составляет «5» зачетных единиц.

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)**
			3
Контактная работа, ак.ч.	*54*		*54*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	36		36
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*99*		*99*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***180***	*180*
	зач.ед.	***5***	*5*

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	Анализ и классификация нормативно-методической базы в области защиты инфор-мации. Модели безопасности операционных систем.	1.1	Основные понятия инфор-мационной безопасности.	ЛК, ЛР
		1.2	Модульная арифметика.	ЛК, ЛР
Раздел 2	Основы криптографии.	2.1	Современные шифры с сим-метричным ключом.	ЛК, ЛР
		2.2	Стандарт шифрования дан-ных.	ЛК, ЛР
		2.3	Криптография с асиммет-ричным ключом.	ЛК, ЛР
Раздел 3	Алгоритмы обмена ключей и протоколы аутентификации.	3.1	Целостность сообщения и установление подлинности сообщения.	ЛК, ЛР
		3.2	Установление подлинности объекта.	ЛК, ЛР
		3.3	Управление ключами.	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.	Компьютер/ноутбук с досту-пом сети Интернет и элек-тронно-образовательной сре-де Университета, браузер, ПО для просмотра PDF, MS Teams.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве ____ шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	ОС Linux/ Windows, Python, Julia. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio.
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.	ОС Linux/ Windows, Python, Julia. Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компью-терную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рож-ков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2020. — 473 с. — (Высшее об-разование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277.
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Ма-тематические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под ре-дакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — (Выс-шее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469567.

Дополнительная литература:

1. Информационная безопасность компьютерных сетей: учебно-методический комплекс / Д.С. Кулябов, А. В. Королькова, М. Н. Геворкян. — Москва: РУДН, 2015. — 64 с.
2. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — Издательство: Горячая линия — Телеком , 2011 г.
3. Лапонина О.Р. «Основы сетевой безопасности: криптографические алгоритмы и про-токолы взаимодействия: учебное пособие», 3-е изд. испр., М. ИНТУИТ.РУ «Интер-нет-Университет Информационных Технологий», БИНОМ. Лаборатория знаний, 2012г., 531с. — URL: http://www.intuit.ru/department/security/networksec/.
4. В. Столлингс «Криптография и защита сетей. Принципы и практика», 2-е изд. 2001г., Издательский дом «Вильямс», 672 с.
5. Б. Шнайер «Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С», 2-е изд. 2003г.
6. М. А. Иванов «Криптографические методы защиты информации в компьютерных си-стемах и сетях», 2001г., «Кудиц-образ», 386с.

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 «Математические основы защиты информации и информационной безопасности».

* - 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 «Математические основы защиты информации и информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

РАЗРАБОТЧИК:

Профессор кафедры теории вероятностей и кибербезопасности		Кулябов Д. С.
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов К. Е.
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой математического моделирования и искусственного интеллекта		Малых М. Д.
Должность, БУП	*Подпись*	*Фамилия И.О.*