

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 27.06.2022 11:51:29

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a9896ae18a

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов»

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:

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)

2022 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Математические основы защиты информации и информационной безопасности» 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): УК-1; УК-2.; ОПК-1; ОПК-2; ПК-2.

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	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

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
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 проектирования и дизайна ИС	ПК-2.3 Знает основы программирования, современные методики тестирования разрабатываемых информационных 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 Б1 ОП ВО.

В рамках ОП ВО 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 ¹
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Введение в компьютерные науки и искусственный интеллект; Архитектура беспроводных сетей; Объектные и распределённые базы данных;	Технологическая (проектно-технологическая) практика; Преддипломная практика
УК-2	Способен управлять проектом на всех этапах его жизненного	Введение в компьютерные науки и искусственный	Технологическая (проектно-технологическая) практика; Преддипломная практика

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики
	цикла	интеллект;	
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	Введение в компьютерные науки и искусственный интеллект; Архитектура беспроводных сетей;	Технологическая (проектно-технологическая) практика; Преддипломная практика
ОПК-2	Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач;	Архитектура беспроводных сетей;	Технологическая (проектно-технологическая) практика; Преддипломная практика
ПК-2	Организационное и технологическое обеспечение проектирования и дизайна ИС	Введение в компьютерные науки и искусственный интеллект; Объектные и распределённые базы данных;	Технологическая (проектно-технологическая) практика; Преддипломная практика

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 ОП ВО

Вид учебной работы	ВСЕГО, ак.ч.	Семестр(-ы)
		3
<i>Контактная работа, ак.ч.</i>	54	54
Лекции (ЛК)	18	18
Лабораторные работы (ЛР)	36	36
Практические/семинарские занятия (СЗ)	-	-
<i>Самостоятельная работа обучающихся, ак.ч.</i>	99	99
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	27	27
Общая трудоемкость дисциплины	ак.ч.	180
	зач.ед.	5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы ²
Раздел 1. Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем	Тема 1.1. Основные понятия информационной безопасности.	ЛК, ЛР
	Тема 1.2. Элементы теории информации и кодирования.	ЛК, ЛР
Раздел 2. Основы криптографии	Тема 2.1. Математические основы криптографии.	ЛК, ЛР
	Тема 2.2. Симметричная криптография.	ЛК, ЛР
	Тема 2.3. Асимметричная криптография.	ЛК, ЛР
Раздел 3. Алгоритмы обмена ключей и протоколы аутентификации	Тема 3.1. Хэш-функции и аутентификация сообщений. Цифровая подпись.	ЛК, ЛР
	Тема 3.2. Алгоритм обмена ключами Диффи–Хеллмана.	ЛК, ЛР
	Тема 3.3. Основные принципы построения защищённых систем.	ЛК, ЛР

2 - заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – 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.
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 обучающихся	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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — 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. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/469567>.

Дополнительная литература:

1. Математические основы защиты информации и информационной безопасности 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. Лапоница О.Р. «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие», 3-е изд. испр., М. ИНТУИТ.РУ «Интернет-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 системах 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 «Лань» <http://e.lanbook.com/>

- 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/модуля³:

1. Курс видеолекций по дисциплине «Математические основы защиты информации и информационной безопасности».

2. Лабораторный практикум по дисциплине «Математические основы защиты информации и информационной безопасности».

3 - 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 система⁴ 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.

РАЗРАБОТЧИКИ:

Профессор кафедры прикладной информатики и теории вероятностей

Должность, БУП



Подпись

Д.С. Кулябов

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей

Наименование БУП



Подпись

К.Е. Самуйлов

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Доцент кафедры информационных технологий

Должность, БУП



Подпись

М.Б. Фомин

Фамилия И.О.

4 - Ом и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.