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:

02.04.02 Фундаментальная информатика и информационные технологии
(код и наименование направления подготовки/специальности)

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

Управление инфокоммуникациями и интеллектуальные системы
(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, УК-7, ОПК-1, ОПК-2, ОПК-4, ПК-1 (в части ПК-1.3), ПК-2 (в части ПК-2.5)

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-2.2 Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.
УК-7	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 полу-	УК-7.1 Знает принципы применения цифровых технологий для сбора, отбора и обобщения информации УК-7.2 Умеет применять цифровые технологии для поиска, обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий УК-7.3 Владеет навыками применения цифровых технологий и методов поиска,

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	ченными 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	обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий
ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.	ОПК-1.1 Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций ОПК-1.3 Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности ОПК-1.2 Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты
ОПК-2	Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.	ОПК-2.1 Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включённого в Единый Реестр Российских программ. ОПК-2.2 Умеет анализировать типовые языки программирования, составлять программы. ОПК-2.3 Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов коммуникации.
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	ОПК-4.1 Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла. ОПК-4.2 Умеет осуществлять управление проектами информационных систем. ОПК-4.3 Имеет практический опыт анализа и интерпретации информационных систем.
ПК-1	Проведение работ по обработке и анализу научно-технической информации и результатов	ПК-1.3 Умеет применять полученные знания в области фундаментальных научных основ математики и информатики, а также решать стандартные задачи собственной

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	исследований.	научно-исследовательской деятельности; умеет решать научные задачи с пониманием существующих подходов к верификации моделей по тематике исследований в соответствии с выбранной методикой. научных семинаров, научно-технических конференций.
ПК-2	Организационное и технологическое обеспечение проектирования и дизайна ИС.	ПК-2.5 Знает основы программирования; современные методики тестирования разрабатываемых информационных систем; современные инструменты и методы верификации программного кода.

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
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 цикла	Введение в компьютерные науки и искусственный интеллект	Технологическая (проектно-технологическая) практика Преддипломная практика
УК-7	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информа-	Введение в компьютерные науки и искусственный интеллект	Технологическая (проектно-технологическая) практика Преддипломная практика

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики	Последующие дисциплины/модули, практики
	цию 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		
ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	Введение в компьютерные науки и искусственный интеллект Архитектура беспроводных сетей	Технологическая (проектно-технологическая) практика Преддипломная практика
ОПК-2	Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности	Архитектура беспроводных сетей	Технологическая (проектно-технологическая) практика Преддипломная практика
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	Архитектура беспроводных сетей	Технологическая (проектно-технологическая) практика Преддипломная практика
ПК-1	Проведение работ по обработке и анализу научно-технической информации и результатов исследований	Введение в компьютерные науки и искусственный интеллект Объектные и распределённые базы данных	Технологическая (проектно-технологическая) практика Преддипломная практика

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики	Последующие дисциплины/модули, практики
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 6 зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		ВСЕГО, ак.ч.	Семестр(-ы)
			1
Контактная работа, ак.ч.		*54*	*54*
в том числе:			
Лекции (**ЛК**)		18	18
Лабораторные работы (**ЛР**)		36	36
Практические/семинарские занятия (**СЗ**)			
Самостоятельная работа обучающихся, ак.ч.		*135*	*135*
Контроль (экзамен/зачет с оценкой), ак.ч.		*27*	*27*
Общая трудоемкость дисциплины	ак.ч.	**216**	**216**
	зач.ед.	**6**	**6**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы[1]
Раздел 1 Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем	Тема 1.1 Основные понятия информационной безопасности. Тема 1.2 Модульная арифметика.	ЛК, ЛР
Раздел 2 Основы криптографии.	Тема 2.1. Современные шифры с симметричным ключом. Тема 2.2 Стандарт шифрования данных (DES). Тема 2.3 Криптография с асимметричным ключом.	ЛК, ЛР

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
Раздел 3 Алгоритмы обмена ключей и протоколы аутентификации.	Тема 3.1 Целостность сообщения и установление подлинности сообщения. Тема 3.2 Установление подлинности объекта. Тема 3.3. Управление ключами.	ЛК, ЛР

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 18 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. 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 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»:

- 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» http://www.studentlibrary.ru
  - ЭБС «Лань» http://e.lanbook.com/
  - ЭБС «Троицкий мост»
- 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 видеолекций по дисциплине «Математические основы защиты информации и информационной безопасности».
2. Лабораторный практикум по дисциплине «Математические основы защиты информации и информационной безопасности».

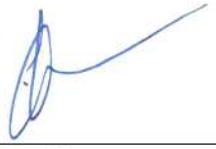
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

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.

РАЗРАБОТЧИКИ:

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

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Наименование БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Должность, БУП	Подпись	Фамилия И.О.