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:

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):

БЕСПРОВОДНЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ И КИБЕРБЕЗОПАСНОСТЬ
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Математические основы защиты информации и информационной безопасности» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается в 1 семестре 1 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)
ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	ОПК-1.1 Обладает фундаментальными знаниями в области прикладной математики, фундаментальной информатики и информационных технологий; ОПК-1.2 Формулирует и решает задачи прикладной математики, фундаментальной информатики и информационных технологий; ОПК-1.3 Определяет и применяет математические и иные методы для решения профессиональных задач;
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 Определяет информационно-коммуникационные технологии, необходимые для решения задач в области профессиональной деятельности; ОПК-4.2 Оценивает риски и угрозы при использовании информационно-коммуникационных технологий, определяет способы и инструменты защиты данных при решении задач в области профессиональной деятельности; ОПК-4.3 Применяет на практике методы и средства защиты информации при ее сборе, хранении, обработке и передаче;

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*
ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий		Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Научно-исследовательская работа; Методы стохастического анализа телекоммуникаций; Нотации моделирования и методы анализа бизнес-процессов; Пакеты символьных вычислений; Высокопроизводительные вычисления;
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности		Научно-исследовательская работа; Криптографические методы защиты информации; Анализ и показатели эффективности кибербезопасности предприятия;

* - 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 «4» 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)**
			1
Контактная работа, ак.ч.	*36*		*36*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	18		18
Практические/семинарские занятия (**СЗ**)	0		0
Самостоятельная работа обучающихся, ак.ч.	*108*		*108*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем.	1.1	Основные понятия информационной безопасности.	Предмет информационной безопасности. Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность. Угрозы информационной безопасности. Каналы утечки информации. Неформальная модель нарушителя. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности. Сигналы, данные и методы получения информации. Свойства информации. Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации. Определение вероятности и основные правила вычисления количества информации. Информационная модель Шеннона. Формулы Шеннона и Хартли. Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования. Метод сжатия по Хаффману. Код Хэмминга. Основные принципы построения защищённых систем. Меры противодействия угрозам безопасности. Принципы построения систем защиты. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа. Системы разграничения доступа.	ЛК, ЛР
		1.2	Модульная арифметика.	Множества и отношения. Бинарные отображения. Основная теорема арифметики. Алгоритм деления в Z. Понятие группы. Изоморфизмы групп. Понятие и свойства колец. Кольцо вычетов. Понятие поля. Поля Галуа. Кольца многочленов. Алгоритм деления в A[X]. Разложение в кольце многочленов. Неприводимые многочлены. Модулярная арифметика. Китайская теорема об остатках. Эллиптические кривые.	ЛК, ЛР
Раздел 2	Основы криптографии.	2.1	Современные шифры с симметричным ключом.	Понятие симметричных алгоритмов шифрования. Обзор классических симметричных алгоритмов. Моноафавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры. Диффузия и коффузия. Схема Файстеля. Алгоритмы генерации	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				псевдослучайных последовательностей.	
		2.2	Стандарт шифрования дан-ных.	Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES. Режимы функционирования блочных шифров. Скремблеры. Виды криптоанализа симметричных алгоритмов.	ЛК, ЛР
		2.3	Криптография с асимметричным ключом.	Особенности систем с открытым ключом. Генерация простых чисел. Тест простоты Миллера–Рабина. Вероятностный тест простоты Соловея–Штрассена. Полиномиальный критерий простоты AKS. Извлечение квадратного корня в конечных полях. Алгоритм RSA.	ЛК, ЛР
Раздел 3	Алгоритмы обмена ключей и протоколы аутентификации.	3.1	Целостность сообщения и установление подлинности сообщения.	Понятие и свойства хэш-функции. Электронная шифровая подпись. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамаля. Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.	ЛК, ЛР
		3.2	Установление подлинности объекта.	Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма. Протокол Kerberos. Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x. Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.	ЛК, ЛР
		3.3	Управление ключами.	Алгоритм обмена ключами Диффи–Хеллмана. Понятие криптографического протокола. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».	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 доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или ЯндексТелемост.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 20 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 компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560426

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, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560804

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. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915

3. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672

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. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560977

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 «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**!

РАЗРАБОТЧИК:

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

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*