Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет»

УТВЕРЖДАЮ
Первый проректор Белорусско-Российского университета

_____ Ю.В. Машин
22 12 2023

Регистрационный № УД-010304/Б.1.О.31/р

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И ПРОЦЕССОВ
(наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Разработка программного обеспечения

Квалификация Бакалавр

	Форма обучения
	Очная
Курс	4
Семестр	8
Лекции, часы	22
Лабораторные работы, часы	22
Экзамен, семестр	8
Контактная работа по учебным занятиям, часы	44
Самостоятельная работа, часы	64
Всего часов / зачетных единиц	108/3

Кафедра-разработчик программы: «Высшая математика»
(название кафедры)

Составители: В.Г. Замураев, канд. физ.-мат. наук, доцент
(И.О. Фамилия, ученая степень, ученое звание)
И.У. Примак, канд. физ.-мат. наук, доцент
(И.О. Фамилия, ученая степень, ученое звание)

Могилев, 2023

Рабочая программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 01.03.04 Прикладная математика № 11 от 10.01.2018,
учебным планом рег. № 010304-2.1 от 28.04.2023.

Рассмотрена и рекомендована к утверждению кафедрой «Высшая математика»
(название кафедры)

28 сентября 2023 г., протокол № 1.

Зав. кафедрой _____ В.Г. Замураев

Одобрена и рекомендована к утверждению Научно-методическим советом Белорусско-Российского университета

20 декабря 2023 г., протокол № 3.

Зам. председателя
Научно-методического совета _____ С.А. Сухоцкий

Рецензент:
Леонид Евгеньевич Старовойтов, доцент кафедры педагогики и психологии учреждения образования «Могилевский государственный областной институт развития образования», кандидат физико-математических наук, доцент

Рабочая программа согласована:

Ведущий библиотекарь О.С. Шуляковская

Начальник учебно-методического
отдела _____ О.Е. Печковская

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель учебной дисциплины

Целью учебной дисциплины является формирование специалистов, умеющих обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач в сфере информационных технологий математические методы и модели.

1.2 Планируемые результаты изучения дисциплины

В результате освоения учебной дисциплины студент должен

знать:
– основные понятия теории информации;
– математические основы моделирования криптосистем;
– основные понятия криптографии;
– основные методы и стандарты шифрования;
уметь:
– применять методы и модели теории информации к решению задач передачи сообщений;
– применять методы и алгоритмы шифрования и дешифрования;
владеть:
– методами и алгоритмами криптографии и криптоанализа;
– навыками творческого аналитического мышления.

1.3 Место учебной дисциплины в системе подготовки студента

Дисциплина относится к Блоку 1 "Дисциплины (модули)"(обязательная часть).
Перечень учебных дисциплин, изучаемых ранее, усвоение которых необходимо для изучения данной дисциплины:
– дискретная математика;
– математическая логика и теория алгоритмов;
– теория вероятностей и случайные процессы;
– математическая статистика;
– случайные процессы;
– математическое моделирование в естествознании, технике и экономике;

Результаты, полученные при изучении дисциплины на лекциях и лабораторных занятиях, будут применены при прохождении преддипломной практики, а также при подготовке выпускной квалификационной работы и в дальнейшей профессиональной деятельности.

1.4 Требования к освоению учебной дисциплины

Освоение данной учебной дисциплины должно обеспечивать формирование следующих компетенций:

Коды формируемых компетенций	Наименования формируемых компетенций
ОПК-2	Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы

	и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надёжность и качество функционирования систем
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
ПК-1	Способен проводить научно-исследовательские разработки при исследовании самостоятельных тем

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Вклад дисциплины в формирование результатов обучения выпускника (компетенций) и достижение обобщенных результатов обучения происходит путём освоения содержания обучения и достижения частных результатов обучения, описанных в данном разделе.

2.1 Содержание учебной дисциплины

Номера тем	Наименование тем	Содержание	Коды формируемых компетенций
Основные понятия теории информации			
1.	Предмет теории информации. Энтропия как мера степени неопределенности. Измерение информации	Предмет теории информации. Определение и свойства энтропии. Энтропия сложной системы. Условная энтропия. Объединение зависимых систем. Определение и свойства информации. Информация об одной системе, содержащаяся в другой системе. Частная информация о системе	ОПК-2, ОПК-3, ПК-1
2.	Энтропия и информация для непрерывных систем	Энтропия для непрерывных систем. Условная энтропия для непрерывных систем. Энтропия объединённой непрерывной системы. Информация для непрерывных систем	ОПК-2, ОПК-3, ПК-1
3.	Приложение теории информации к задачам передачи сообщений	Виды информации. Экономность кода. Наилучший равномерный код. Коды Шеннона-Фано и Хафмена. Блоковые коды. Обобщение для k-ичных кодов. Словарно-ориентированные методы кодирования. Метод Лемпелла-Зива. Сжатие информации с потерями. Общая схема передачи сообщений по линии связи. Пропускная способность линии связи	ОПК-2, ОПК-3, ПК-1
4.	Передача сообщений при наличии помех. Коды, обнаруживающие и исправляющие ошибки	Математическое описание линии связи с помехами. Пропускная способность канала с помехами. Избыточность кодовых обозначений. Прием проверки на четность для обнаружения одиночной ошибки. Прием проверки на четность для обнаружения одной или двух ошибок. Матричное кодирование. Алгебраическое кодирование. Циклические коды	ОПК-2, ОПК-3, ПК-1
Моделирование криптосистем			
5.	Математические основы моделирования	Делители и простые числа. НОД. Основная теорема арифметики. Алгоритм Евклида. Расширенный алгоритм Евклида. Малая теорема Ферма. Функция Эйлера. Сравнение и его свойства. Системы вычетов. Малая теорема Ферма. Алгоритм быстрого возведение в степень по модулю. Сравнение первой степени. Линейные Диофантовы уравнения. Китайская теорема об остатках.	ОПК-2, ОПК-3, ПК-1
6.	Математические основы моделирования	Проверка чисел на простоту: детерминированные и вероятностные тесты, тест Ферма, числа Кармайкла, тест Миллера — Рабина, вероятностный тест простоты Соловея–Штрассена. Генерация простых чисел: метод пробных делений, решето Эратосфена, простые числа Мерсенна, символы Лежандра и Якоби. Факторизация целого числа: формулировка задачи и методы решения (Ферма и Полларда).	ОПК-2, ОПК-3, ПК-1
7.	Математические основы моделирования	Дискретные логарифмы. Понятия случайной и псевдослучайной последовательностей. Методы получения псевдослучайной последовательности (ЛКГ, Фибоначчи, BBS).	ОПК-2, ОПК-3, ПК-1

8.	Основные понятия криптографии. Шифры подстановки	Основные понятия и определения. Модель традиционного шифрования. Классификация криптоалгоритмов. Криптоанализ и его методы. Шифрование на основе методов подстановки: моноалфавитные шифры (Цезаря, Плейфера, Хила), полиалфавитные шифры (Вижинера, Вирнама), криптоанализ (перебор ключей, частотный анализ).	ОПК-2, ОПК-3, ПК-1
9.	Шифрование на основе методов перестановки	Методы перестановки (шифры одинарной, множественной, маршрутной перестановок). Блочные шифры. Шифр Файстеля (диффузия и конфузия, структура шифра, алгоритм дешифрования). Композиция методов шифрования. Криптоанализ.	ОПК-2, ОПК-3, ПК-1
10.	Стандарт шифрования DES	Структура DES. Схема алгоритма. Процесс шифрования (начальная подготовка блока данных, основной цикл, конечная обработка блока данных). Дешифрование DES. Криптоанализ (дифференциальный, линейный).	ОПК-2, ОПК-3, ПК-1
11.	Криптосистемы с открытым ключом	Общая схема шифрования с открытым ключом. Особенности применения криптосистем с открытым ключом. Алгоритм шифрования RSA (структура, вычисление ключей, криптоанализ). Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм Эль-Гамаля. Схемы RSA и Эль-Гамаля для формирования и проверки электронной цифровой подписи (ЭЦП).	ОПК-2, ОПК-3, ПК-1

2.2 Учебно-методическая карта учебной дисциплины

№ недели	Лекции (наименование тем)	Часы	Лабораторные занятия	Часы	Самостоятельная работа, часы	Форма контроля знаний	Баллы (max)
Модуль 1							
1	Лекция № 1. Предмет теории информации. Энтропия как мера степени неопределенности. Измерение информации	2	Л. р. 1. Энтропия и информация	2	2		
2	Лекция № 2. Энтропия и информация для непрерывных систем	2	Л. р. 2. Энтропия и информация для непрерывных систем	2	2		
3	Лекция № 3. Приложение теории информации к задачам передачи сообщений	2	Л. р. 3. Передача сообщений	2	2		
4	Лекция № 4. Передача сообщений при наличии помех. Коды, обнаруживающие и исправляющие ошибки	2	Л. р. 4. Передача сообщений при наличии помех	2	2		
5	Лекция № 5. Математические основы моделирования	2	Л. р. 5. Коды, обнаруживающие и исправляющие ошибки	2	4	КТ	30
6	Лекция № 6. Математические основы моделирования	2	Л. р. 6. Математические основы моделирования	2	4	ПКУ	30
Модуль 2							
7	Лекция № 7. Математические основы моделирования	2	Л. р. 7. Математические основы моделирования	2	4		
8	Лекция № 8. Основные понятия криптографии. Шифры подстановки	2	Л. р. 8. Шифры подстановки	2	2		
9	Лекция № 9. Шифрование на основе методов перестановки	2	Л. р. 9. Шифры подстановки	2	2		
10	Лекция № 10. Стандарт шифрования DES	2	Л. р. 10. Шифры подстановки	2	2	КТ	30
11	Лекция № 11. Криптосистемы с открытым ключом	2	Л. р. 11. Криптосистемы с открытым ключом	2	2	ПКУ	30
12-14					36	ПА (экзамен)	40
	Итого	22		22	64		100

Принятые обозначения
Текущий контроль –
КТ – компьютерное тестирование;
ПКУ – промежуточный контроль успеваемости;
ПА – промежуточная аттестация.

Итоговая оценка определяется как сумма текущего контроля и промежуточной аттестации и соответствует баллам:

Экзамен

Оценка	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Баллы	87-100	65-86	51-64	0-50

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении дисциплины используется модульно-рейтинговая система оценки знаний студентов. Применение форм и методов проведения занятий при изучении различных тем курса представлено в таблице.

№ п/п	Форма проведения занятия	Вид аудиторных занятий		Всего часов
		Лекции	Лабораторные работы	
1	Традиционные		1-11	22
2	Мультимедиа	1-11		22
	ИТОГО	22	22	44

4 ОЦЕНОЧНЫЕ СРЕДСТВА

Используемые оценочные средства по учебной дисциплине представлены в таблице и хранятся на кафедре.

№ п/п	**Вид оценочных средств**	**Количество комплектов**
1	Вопросы к экзамену	1
2	Экзаменационные билеты	1
3	Тестовые (электронные) программы для оценки знаний студентов	1
4	Тестовые задания, формирующие фонд оценочных средств	1

5 МЕТОДИКА И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ СТУДЕНТОВ

5.1 Уровни сформированности компетенций

№ п/п	**Уровни сформированности компетенции**	**Содержательное описание уровня**	**Результаты обучения**
Компетенция ОПК-2. Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надёжность и качество функционирования систем			
Код и наименование индикатора достижения компетенции. ИОПК-2.19 Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач в сфере информационных технологий математические модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надёжность и качество функционирования систем			
1	Пороговый уровень	Базовые знания в объеме рабочей программы (знание определений	Умение решать типовые исследовательские задачи,

		основных понятий), умение решать типовые задачи под руководством преподавателя.	требующее применять в знакомой ситуации известные факты, стандартные приемы, распознавать математические объекты и свойства, применять известные алгоритмы и технические навыки.
2	Продвинутый уровень	Полные знания в объеме рабочей программы, правильное использование терминологии, способность самостоятельно решать типовые задачи учебной дисциплины.	Умение решать исследовательские и проектные задачи, которые не являются типичными, выходят за рамки известного лишь в небольшой степени, посредством применения стандартных математических методов и моделей.
3	Высокий уровень	Систематизированные, глубокие и полные знания в объеме рабочей программы, точное использование научной терминологии и свободное владение инструментарием учебной дисциплины, умение анализировать и применять теоретические знания при самостоятельном решении типовых учебных задач и задач повышенной сложности, способность делать обоснованные выводы.	Умение решать исследовательские и проектные задачи, которые требуют определенной интуиции, размышлений и творчества в выборе математических методов и моделей, интегрирования знаний из разных математических дисциплин, самостоятельная разработка математических моделей.
Компетенция ОПК-3. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности			
Код и наименование индикатора достижения компетенции. ИОПК-3.5 Способен применять знание математических основ теории информационных систем и процессов при изучении принципов работы современных информационных технологий			
1	Пороговый уровень	Базовые знания в объеме рабочей программы (знание определений основных понятий), умение решать типовые задачи под руководством преподавателя.	Умение решать типовые исследовательские задачи, требующее применять в знакомой ситуации известные факты, стандартные приемы, распознавать математические объекты и свойства, применять известные алгоритмы и технические навыки.
2	Продвинутый уровень	Полные знания в объеме рабочей программы, правильное использование терминологии, способность самостоятельно решать типовые задачи учебной дисциплины.	Умение решать исследовательские и проектные задачи, которые не являются типичными, выходят за рамки известного лишь в небольшой степени, посредством применения стандартных математических

			методов и моделей.
3	Высокий уровень	Систематизированные, глубокие и полные знания в объеме рабочей программы, точное использование научной терминологии и свободное владение инструментарием учебной дисциплины, умение анализировать и применять теоретические знания при самостоятельном решении типовых учебных задач и задач повышенной сложности, способность делать обоснованные выводы.	Умение решать исследовательские и проектные задачи, которые требуют определенной интуиции, размышлений и творчества в выборе математических методов и моделей, интегрирования знаний из разных математических дисциплин, самостоятельная разработка математических моделей.
Компетенция ПК-1. Способен проводить научно-исследовательские разработки при исследовании самостоятельных тем			
Код и наименование индикатора достижения компетенции. ИПК-1.17 Способен применять знание методов математического моделирования информационных систем и процессов при проведении научно-исследовательских разработок			
1	Пороговый уровень	Базовые знания в объеме рабочей программы (знание определений основных понятий), умение решать типовые задачи под руководством преподавателя.	Умение решать типовые исследовательские задачи, требующее применять в знакомой ситуации известные факты, стандартные приемы, распознавать математические объекты и свойства, применять известные алгоритмы и технические навыки.
2	Продвинутый уровень	Полные знания в объеме рабочей программы, правильное использование терминологии, способность самостоятельно решать типовые задачи учебной дисциплины.	Умение решать исследовательские и проектные задачи, которые не являются типичными, выходят за рамки известного лишь в небольшой степени, посредством применения стандартных математических методов и моделей.
3	Высокий уровень	Систематизированные, глубокие и полные знания в объеме рабочей программы, точное использование научной терминологии и свободное владение инструментарием учебной дисциплины, умение анализировать и применять теоретические знания при самостоятельном решении типовых учебных задач и задач повышенной сложности, способность делать обоснованные выводы.	Умение решать исследовательские и проектные задачи, которые требуют определенной интуиции, размышлений и творчества в выборе математических методов и моделей, интегрирования знаний из разных математических дисциплин, самостоятельная разработка математических моделей.

5.2 Методика оценки знаний, умений и навыков студентов

Результаты обучения	Оценочные средства
Компетенция ОПК-2. Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надёжность и качество функционирования систем	
Пороговый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Продвинутый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Высокий уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Компетенция ОПК-3. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
Пороговый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Продвинутый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Высокий уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Компетенция ПК-1. Способен проводить научно-исследовательские разработки при исследовании самостоятельных тем	
Пороговый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Продвинутый уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания
Высокий уровень	Вопросы к экзамену Экзаменационные билеты Тестовые (электронные) программы для оценки знаний студентов Тестовые задания

5.4 Критерии оценки лабораторных работ

Оценка эффективности усвоения студентом материала, пройденного на лабораторных работах, осуществляется с помощью компьютерного тестирования. Каждый тест оценивается по шкале от 0 до 30 баллов. Количество баллов, полученных студентом за тест равно сумме баллов за каждое задание.

5.6 Критерии оценки экзамена

Итоговая оценка на экзамене по пятибалльной системе определяется как сумма баллов промежуточного контроля успеваемости и промежуточной аттестации (экзамена) и

соответствует суммарным баллам:

Оценка	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Баллы	87-100	65-86	51-64	0-50

При этом промежуточный контроль успеваемости оценивается до 60 баллов, а промежуточная аттестация (экзамен) оценивается до 40 баллов. Экзаменационный билет состоит из 4 вопросов (2 теоретических вопроса и 2 задачи), за каждое задание можно набрать до 10 баллов.

Для экзамена.

Оценка **«отлично»**, выставляется за: систематизированные, глубокие и полные знания в объеме рабочей программы, точное использование научной терминологии и свободное владение инструментарием учебной дисциплины, умение анализировать и применять теоретические знания при самостоятельном решении типовых учебных задач и задач повышенной сложности, способность делать обоснованные выводы.

Оценка **«хорошо»**, выставляется за: полные знания в объеме рабочей программы, правильное использование терминологии, способность самостоятельно решать типовые задачи учебной дисциплины.

Оценка **«удовлетворительно»**, выставляется за: обладание базовыми знаниями (владеет терминологией, знает определения понятий) в объеме рабочей программы достаточными для усвоения последующих дисциплин, умение решать простейшие типовые задачи.

Оценка **«неудовлетворительно»**, выставляется за: фрагментарные знания по базовым вопросам в объеме рабочей программы, недостаточными для усвоения последующих дисциплин, неуверенное использование терминологии, неумение решать типовые задачи.

6 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Самостоятельная работа студентов (СРС) направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СРС включает следующие виды самостоятельной работы студентов:

конспектирование;

решение задач и упражнений по образцу;

работа с лекционными материалами, включая основную и дополнительную литературу, которые представлены в пунктах 7.1 и 7.2;

работа с материалами курса, вынесенными на самостоятельное изучение;

работа со справочной литературой;

подготовка к аудиторным занятиям и контрольным работам;

подготовка к экзамену.

Для СРС рекомендуется использовать источники, приведенные в п. 7.

Перечень методических указаний приведен в п. 7.4.1 и они хранятся в кабинете математики (к. 405). Кроме того, их электронные варианты представлены в университетской сети Интернет по адресу: eco.bru.by.

По адресу cdo.bru.by (учебные материалы), находится разработанный на кафедре электронный учебно-методический комплекс (ЭУМК), который включает:

- курс лекций;
- методические рекомендации для практических занятий;
- примеры контрольных заданий
- вопросы к экзаменам,
- образцы экзаменационных билетов;
- список литературы.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1 Основная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с.	нет	URL: https://znanium.com/catalog/product/1899016
2	Приходько, А. И. Теория информации. Лабораторный практикум в MATLAB : учебное пособие / А. И. Приходько. - Москва ; Вологда : Инфра-Инженерия, 2022. - 108 с.	Рекомендовано УМО РАЕ по классическому университетскому и техническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки: 11.03.02 "Инфокоммуникационные технологии и системы связи", 11.03.01 "Радиотехника"	URL: https://znanium.com/catalog/product/1902595

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	Душин, В. К. Теоретические основы информационных процессов и систем / Душин В.К., - 5-е изд. - Москва :Дашков и К, 2018. - 348 с.	нет	URL: https://znanium.com/catalog/product/450784
2	Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.	Рекомендовано Сибирским региональным учебно-методическим центром высшего профессионального образования для межвузовского использования в качестве учебного пособия для студентов, обучающихся по специальности 090102 "Компьютерная безопасность" и направлениям подготовки 090900 "Информационная безопасность" и 010200 "Математика и компьютерные науки" от 5 июля 2010 года	URL: https://znanium.com/catalog/product/441493
3	Теория чисел в криптографии : учебное пособие / В. А. Орлов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева. - Москва : МГТУ им. Баумана, 2011. - 224 с.	Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению "Информатика и вычислительная техника"	URL: https://znanium.com/catalog/product/2017285

7.3 Перечень ресурсов сети Интернет по изучаемой дисциплине

Znanium.com, biblio.bru.by

7.4 Перечень наглядных и других пособий, методических рекомендаций по проведению учебных занятий, а также методических материалов к используемым в образовательном процессе техническим средствам

7.4.1 Методические рекомендации

1. Математическое моделирование информационных систем и процессов. Методические рекомендации к лабораторным работам для студентов направления подготовки 01.03.04 «Прикладная математика» очной формы обучения / составители В.Г. Замураев, И.У. Примак. – Могилев: Белорус.-Рос. ун-т, 2024. (Электронный вариант).

7.4.2 Информационные технологии

Мультимедийные презентации:

Предмет теории информации. Энтропия как мера степени неопределенности. Измерение информации (лекция № 1).

Энтропия и информация для непрерывных систем (лекция № 2).

Приложение теории информации к задачам передачи сообщений (лекция № 3).

Передача сообщений при наличии помех. Коды, обнаруживающие и исправляющие ошибки (лекция № 4).

Математические основы моделирования (лекции №№ 5-7).

Основные понятия криптографии. Шифры подстановки (лекция № 8).

Шифрование на основе методов перестановки (лекция № 9).

Стандарт шифрования DES (лекция № 10).

Криптосистемы с открытым ключом (лекция № 11).

7.4.3 Перечень программного обеспечения, используемого в образовательном процессе

Acrobat Reader DC, Apache OpenOffice, система управления курсами Moodle (свободное программное обеспечение).

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины содержится в паспорте лабораторий ауд.405, рег. номер ПУЛ-4.535-405/1-23 и ауд.233, рег. номер ПУЛ-4.535-233/1-23.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

ИНФОРМАЦИОННЫХ СИСТЕМ И ПРОЦЕССОВ

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Направление подготовки 01.03.04 Прикладная математика
Направленность (профиль) Разработка программного обеспечения

	Форма обучения
	Очная
Курс	4
Семестр	8
Лекции, часы	22
Лабораторные работы, часы	22
Экзамен, семестр	8
Контактная работа по учебным занятиям, часы	44
Самостоятельная работа, часы	64
Всего часов / зачетных единиц	108/3

1. Цель учебной дисциплины.
Целью учебной дисциплины является формирование специалистов, умеющих обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач в сфере информационных технологий математические методы и модели.

2. Планируемые результаты изучения дисциплины.
В результате освоения учебной дисциплины студент должен
знать:
– основные понятия теории информации;
– математические основы моделирования криптосистем;
– основные понятия криптографии;
– основные методы и стандарты шифрования;
уметь:
– применять методы и модели теории информации к решению задач передачи сообщений;
– применять методы и алгоритмы шифрования и дешифрования;
владеть:
– методами и алгоритмами криптографии и криптоанализа;
– навыками творческого аналитического мышления.

3. Требования к освоению учебной дисциплины
Освоение данной учебной дисциплины должно обеспечивать формирование следующих компетенций:
ОПК-2 Способен обоснованно выбирать, дорабатывать и применять для решения исследовательских и проектных задач математические методы и модели, осуществлять проверку адекватности моделей, анализировать результаты, оценивать надёжность и качество функционирования систем;
ОПК-3 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
ПК-1 Способен проводить научно-исследовательские разработки при исследовании самостоятельных тем.

4. Образовательные технологии: традиционные, мультимедиа.