

УТВЕРЖДАЮ
Первый проректор, проректор по
УР

_____ А.Е. Рудин

«28» 06 2022 года

Рабочая программа дисциплины

Б1.О.02 Специальные главы математики

Учебный план: 2022-2023 09.04.02 ВШПМ Цифр тех в медиаком и диз ОО №2-1-57.plx

Кафедра: **6** Высшей математики и информатики

Направление подготовки:
(специальность) 09.04.02 Информационные системы и технологии

Профиль подготовки: Цифровые технологии в медиакоммуникациях и дизайне
(специализация)

Уровень образования: магистратура

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоём- кость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
1	УП	17	51	49	27	4	Экзамен
	РПД	17	51	49	27	4	
Итого	УП	17	51	49	27	4	
	РПД	17	51	49	27	4	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 917

Составитель (и):

кандидат физико-математических наук, Доцент

Жихарева
Аркадьевна

Алена

От кафедры составителя:

Заведующий кафедрой высшей математики и информатики

Жихарева
Аркадьевна

Алена

От выпускающей кафедры:

Заведующий кафедрой

Горина
Владимировна

Елена

Методический отдел:

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Сформировать компетенции обучающихся в области построения и применения базовых алгоритмов обработки информации и основных криптографических протоколов

1.2 Задачи дисциплины:

- Познакомить обучающихся с основными математическими структурами, лежащими в основе информационных технологий,
- Познакомить обучающихся с базовыми алгоритмами обработки информации,
- Выработать практические навыки обучающихся в применении базовых алгоритмов обработки информации

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Дисциплина базируется на компетенциях сформированных на предыдущем уровне образования

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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;
Знать: – Основные принципы проектирования информационных систем
Уметь: - Использовать основные алгоритмы обработки информации и криптографические протоколы
Владеть: - Навыками реализации основных протоколов обработки информации
ОПК-7: Способен разрабатывать и применять математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений;
Знать: - Методы реализации криптографических протоколов
Уметь: - осуществлять математическую постановку задач в области информационных технологий
Владеть: – Навыками решений задач с использованием симметричной криптографии

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)			
Раздел 1. Математические основы информатики	1					Д
Тема 1. Основные алгебраические структуры: Группы, кольца, поля.		2	4	3		
Тема 2. Теоретико-числовые функции. Теоремы Ферма и Эйлера.			4	4		
Тема 3. Элементы теории чисел. Модулярная арифметика.		1	4	3		
Тема 4. Основы комбинаторики		1	4	5	ИЛ	
Раздел 2. Алгоритмы обработки информации						Д
Тема 5. Кодирование информации и его задачи.		2	4	3		
Тема 6. Коды Фано, Хаффмена и Хэмминга.		2	5	4	ИЛ	
Тема 7. Коды Зива-Лемпеля и BPE.		1	5	3		
Тема 8. Алгоритмы MTF, BWT, RLE.		2	5	4		
Тема 9. Алгоритмы сортировки		1	4	4		Д
Раздел 3. Основные криптографические протоколы						
Тема 10. Основные задачи криптографии. Криптография с открытым ключом.	2	4	5	ГД		
Тема 11. Протокол RSA, цифровая подпись, аутентификация пользователя.	2	4	6			

Тема 12. Рюкзачные алгоритмы		1	4	5		
Итого в семестре (на курсе для ЗАО)		17	51	49		
Консультации и промежуточная аттестация (Экзамен)		2,5		24,5		
Всего контактная работа и СР по дисциплине		70,5		73,5		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ОПК-1	Рассказывает о математическом аппарате взаимодействия информационных процессов и технологий. Излагает принципы обработки данных в специальном ПО. Применяет современные методы научных исследований для формирования суждений и выводов по проблемам информационных технологий и систем Проводит логико-методологический анализ научного исследования и его результатов	Вопросы для устного собеседования. Практическое задание
ОПК-7	Излагает методы реализации криптографических протоколов. Осуществляет математическую постановку задач в области информационных технологий	Вопросы для устного собеседования. Практическое задание
	Демонстрирует навык решения задач с использованием симметричной криптографии	

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области, умение использовать теоретические знания для решения практических задач. Учитываются баллы, накопленные в течение семестра	
4 (хорошо)	Ответ полный и правильный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но допущены в ответах несущественные ошибки, которые устраняются только в результате собеседования Учитываются баллы, накопленные в течение семестра	
3 (удовлетворительно)	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. Учитываются баллы, накопленные в течение семестра	

2 (неудовлетворительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные существенные ошибки. Не учитываются баллы, накопленные в течение семестра	
-------------------------	---	--

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 1	
1	Целые числа. Наибольший общий множитель, алгоритм Евклида.
2	Простые числа. Основная теорема арифметики
3	Сравнения. Модулярная арифметика
4	Группы.
5	Кольца, поля. Поля конечной характеристики.
6	Кольцо многочленов. Алгоритм деления, приводимые и неприводимые многочлены
7	Фактор-кольцо.
8	Конечные поля.
9	Функция Эйлера, ее свойства.
10	Теоремы Ферма и Эйлера.
11	Алгоритм шифрования RSA.
12	Кодирование как способ представления информации. Кодирование с минимальной избыточностью
13	Код Фано, код Хаффмена
14	Самокорректирующиеся коды. Код Хэмминга.
15	Алгоритмы MTF и BWT.
16	Код Зива-Лемпеля.
17	Основные задачи криптографии

18	Криптография с открытым ключом. Однонаправленные функции, функции с секретом
19	Протокол идентификации Шнорра.
20	Протокол «подбрасывание монеты по телефону».
21	Протокол разделения секрета.
22	Криптосистема без передачи ключей.
23	Задача о рюкзаке и рюкзачные алгоритмы
24	Аутентификация. Цифровая подпись.
25	Идентификация пользователя.
26	Алгоритмы сортировки
27	Основные объекты комбинаторики: размещения, перестановки, сочетания.

5.2.2 Типовые тестовые задания

- Опишите группу симметрии куба, у которого три грани, примыкающие к одной вершине, окрашены в зеленый цвет, остальные – в красный.
- Умножить 212 на 122 в 3-ичной числовой системе.
- Разделить 40122 на 126 в 7-ичной числовой системе.
- Найти НОД(1547, 560).
- Представить 7 как целочисленную линейную комбинацию чисел 1547 и 560.
- Опишите все решения модулярного уравнения $3x=4 \pmod{7}$.
- Найдите минимальное положительное решение сравнения $x=2 \pmod{3}$.
- Пусть $F(x)=X^4+X^3+X^2+1$, $g(X)=X^3+1$ – полиномы с коэффициентами в поле F_2 . Найти НОД($F(X)$, $g(X)$) с помощью алгоритма Евклида.
- Вычислить значение функции Эйлера с аргументом 200.

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

- Написать скрипт на MATLAB для реализации кода Фано.
- Написать скрипт на MATLAB для реализации кода Хаффмена.
- Написать скрипт на MATLAB для реализации алгоритма BWT.
- Написать скрипт на MATLAB для реализации алгоритма k-Sort Transform.

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная Письменная Компьютерное тестирование Иная

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Выполняет текущие задания по дисциплине.

Выступление с реферативным сообщением на предложенную преподавателем тему.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Горячкин, О. В.	Теория информации и кодирования. Часть 1. Теория потенциальной помехоустойчивости	Самара: Поволжский государственный университет телекоммуникаций и информатики	2017	http://www.iprbookshop.ru/77235.html
Горячкин, О. В.	Теория информации и кодирования. Часть 2	Самара: Поволжский государственный университет телекоммуникаций и информатики	2017	http://www.iprbookshop.ru/75413.html

Дехтярь, М. И.	Дискретная математика	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	http://www.iprbookshop.ru/94851.html
Воропаева, Л. В., Башкинова, Е. В., Саушкин, М. Н.	Кодирование числовых данных	Самара: Самарский государственный технический университет, ЭБС АСВ	2021	https://www.iprbookshop.ru/118944.html

6.1.2 Дополнительная учебная литература				
Громов, Ю. Ю., Иванова, О. Г., Кулаков, Ю. В., Гриднев, В. А., Однолько, В. Г.	Дискретная математика	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ	2012	http://www.iprbookshop.ru/63845.html
Бекарева, Н. Д.	Дискретная математика	Новосибирск: Новосибирский государственный технический университет	2019	https://www.iprbookshop.ru/98701.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

Информационная система «Единое окно доступа к образовательным ресурсам. Раздел.

Информатика и информационные технологии» [Электронный ресурс].

URL: http://window.edu.ru/catalog/?p_rubr=2.2.75.6

Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: <http://www.iprbookshop.ru/>

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows

MATLAB

6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска