|  |  |
| --- | --- |
| Министерство науки и высшего образования Российской Федерации  Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)» | |
|  | УТВЕРЖДАЮ  Директор Таганрогского института имени А.П. Чехова (филиала)  РГЭУ (РИНХ)  \_\_\_\_\_\_\_\_\_\_\_\_\_ Голобородько А.Ю.  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г. |
|  |
|  |  |
| **Рабочая программа дисциплины**  **Абстрактная и компьютерная алгебра** | |
|  |  |
| направление 44.03.05 Педагогическое образование (с двумя профилями подготовки)  направленность (профиль) 44.03.05.29 Математика и Информатика | |
|  |  |
| Для набора \_\_\_\_\_\_\_\_\_\_ года | |
|  |  |
| Квалификация  Бакалавр | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| УП: 44.03.05.29-18-5-МИ.plx | | | | | | | | |  |  | стр. 2 | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | КАФЕДРА |  | **информатики** | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Распределение часов дисциплины по семестрам** | | | | | | |  |  |  |  |  |
|  | Семестр  (<Курс>.<Семестр на курсе>) | | | **9 (5.1)** | | Итого | |  |  |  |  |  |
|  | Недель | | | 12 | |  |  |  |  |  |
|  | Вид занятий | | | УП | РП | УП | РП |  |  |  |  |  |
|  | Лекции | | | 20 | 20 | 20 | 20 |  |  |  |  |  |
|  | Лабораторные | | | 34 | 34 | 34 | 34 |  |  |  |  |  |
|  | Итого ауд. | | | 54 | 54 | 54 | 54 |  |  |  |  |  |
|  | Кoнтактная рабoта | | | 54 | 54 | 54 | 54 |  |  |  |  |  |
|  | Сам. работа | | | 54 | 54 | 54 | 54 |  |  |  |  |  |
|  | Часы на контроль | | | 36 | 36 | 36 | 36 |  |  |  |  |  |
|  | Итого | | | 144 | 144 | 144 | 144 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **ОСНОВАНИЕ** | | | | | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Учебный план утвержден учёным советом вуза от 26.04.2022 протокол № 9/1.      Программу составил(и): д-р техн. наук, Зав. каф., Ромм Яков Евсеевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Зав. кафедрой: Тюшнякова И. А. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| УП: 44.03.05.29-18-5-МИ.plx | | |  |  |  |  |  | стр. 3 |
|  |  |  |  |  |  |  |  |  |
| **1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ** | | | | | | | | |
| 1.1 | Формирование знаний основ классических и компьютерных методов высшей алгебры; | | | | | | | |
| 1.2 | освоение базовых элементов теории групп; формирование системных знаний в области абстрактной и компьютерной алгебры; знание методов представления на компьютере классических алгебраических структур, границ применимости символьных вычислений на компьютере; | | | | | | | |
| 1.3 | освоение математических пакетов решения базовых задач, относящихся к компьютерной алгебре; формирование знания математических основ кодирования и защиты информации; | | | | | | | |
| 1.4 | знание альтернативных компьютерных методов решения задач высшей алгебры; формирование с этой целью углубленного понимания основ информатики и программирования в области преобразования и упорядочения числовых данных; знание методов исследования и решения задач в области высшей алгебры, целесообразных при решении профессиональных задач. | | | | | | | |
|  |  |  |  |  |  |  |  |  |
| **2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ** | | | | | | | | |
| **ПК-7:способностью организовывать сотрудничество обучающихся, поддерживать их активность, инициативность и самостоятельность, развивать творческие способности** | | | | | | | | |
| **СК-9:способностью использовать математический аппарат, методологию программирования и современные компьютерные технологии для решения практических задач получения, хранения, обработки и передачи информации** | | | | | | | | |
| **СК-10:способностью владеть современными формализованными математическими, информационно-логическими и логико-семантическими моделями и методами представления, сбора и обработки информации** | | | | | | | | |
| **СК-11:способностью реализовывать аналитические и технологические решения в области программного обеспечения и компьютерной обработки информации** | | | | | | | | |
|  |  |  |  |  |  |  |  |  |
| **В результате освоения дисциплины обучающийся должен:** | | | | | | | | |
| **Знать:** | | | | | | | | |
| способы представления на компьютере классических алгебраических структур, границы применимости символьных вычислений на компьютере; базовые методы перечисления конечных алгебраических объектов; основные методы и алгоритмы компьютерной алгебры; основные методы работы с многочленами в системе компьютерной алгебры; компьютерные методы разложения многочленов на неприводимые множители, основанные на сортировке; математические основы кодирования и защиты информации. | | | | | | | | |
| **Уметь:** | | | | | | | | |
| решать с использованием математических пакетов базовые задачи, относящиеся к компьютерной алгебре; применять основные алгоритмы, реализованные в системе компьютерной алгебры, для решения задач теории чисел; применять основные алгоритмы, реализованные в системе компьютерной алгебры, для решения задач факторизации многочленов; строить разложение многочленов произвольной степени на неприводимые множители на основе устойчивой адресной сортировки; восстанавливать коэффициенты многочлена по его корням для многочлена произвольной степени; воспроизводить базовые элементы алгоритмов кодирования и защиты информации. | | | | | | | | |
| **Владеть:** | | | | | | | | |
| компьютерным решением задач высшей алгебры в связи с символьными вычислениями, теорией чисел и защитой информации. | | | | | | | | |
|  |  |  |  |  |  |  |  |  |
| **3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ** | | | | | | | | |
| **Код занятия** | | **Наименование разделов и тем /вид занятия/** | | **Семестр / Курс** | **Часов** | **Компетен-**  **ции** | **Литература** | |
|  | | **Раздел 1. Символьные вычисления на компьютере. Предмет компьютерной алгебры.** | |  |  |  |  | |
| 1.1 | | Предмет компьютерной алгебры. Основные формы и представления алгебраических объектов и выражений на компьютере. Символьные вычисления на компьютере.  План:  1. Предмет компьютерной алгебры.  2. Основные формы и представления алгебраических объектов и выражений на компьютере.  3. Символьные вычисления на компьютере.  4. Алгоритмическая неразрешимость проблемы тождества слов в основных алгебраических структурах, ее значение для компьютерной алгебры.  5. Математические пакеты для решения базовых задач компьютерной алгебры. /Лек/ | | 9 | 6 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| УП: 44.03.05.29-18-5-МИ.plx | |  |  |  |  |  | стр. 4 |
| 1.2 | Предмет и задачи компьютерной алгебры.  Примеры символьных вычислений на компьютере. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 1.3 | Методы перечисления конечных алгебраических объектов.  Работа с многочленами в системе компьютерной алгебры. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 1.4 | Примеры реализации базовых алгоритмов на графах. /Лаб/ | | 9 | 2 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 1.5 | Самостоятельное работа в системе компьютерной алгебры /Ср/ | | 9 | 14 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
|  | **Раздел 2. Основные структуры алгебры. Группы, кольца, поля.** | |  |  |  |  | |
| 2.1 | Основные структуры алгебры. Группы, кольца, поля.  План:  1. Группы, кольца, поля. Элементы теории делимости в кольцах целых чисел и многочленов. Алгоритм Эвклида.  2. Элементы теории сравнений. Теорема Эйлера. Вычеты.  3. Группы подстановок. Выполнимость тождеств в конечных алгебраических структурах.  /Лек/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 2.2 | Арифметика целых чисел. Сравнение, сложение, вычитание и умножение целых чисел в компьютерной алгебре. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 2.3 | Сравнения. Вычеты. Группы подстановок. Выполнимость тождеств в конечных алгебраических структурах. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
| 2.4 | Самостоятельное изучение основных структур алгебры. /Ср/ | | 9 | 16 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2Л2.1 | |
|  | **Раздел 3. Алгебраические основы кодирования и защиты информации** | |  |  |  |  | |
| 3.1 | Алгебраические основы кодирования и защиты информации  План:  1. Простые числа Мерсенна. Классические и современные алгоритмы факторизации натуральных чисел.  2. Метод Ферма, метод Моррисона-Бриллхарта, метод квадратичного решета.  3. Проблема надежности шифрования с открытым ключом.  4. Методы алгебры и теории чисел как основа криптосистем. /Лек/ | | 9 | 6 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2 Л1.1Л2.1 Л2.2 | |
| 3.2 | Простые числа. Бесконечность множества простых чисел. Методы генерации простых чисел. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2 Л1.1Л2.1 Л2.2 | |
| 3.3 | Алгоритмы факторизации натуральных чисел. Простейшие примеры кодирования и декодирования. Примеры криптосистем. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2 Л1.1Л2.1 Л2.2 | |
| 3.4 | Подготовка реферата / доклада по теме. /Ср/ | | 9 | 12 | СК-9 СК-10 СК-11 ПК-7 | Л1.3 Л1.2 Л1.1Л2.1 Л2.2 | |
|  | **Раздел 4. Работа с многочленами над конечными полями и полем рациональных чисел.** | |  |  |  |  | |
| 4.1 | Факторизация многочленов над конечным полем. Разложение многочленов на неприводимые множители.  План:  1. Факторизация многочленов над полем рациональных чисел.  2. Алгоритм сортировки для программного разложения многочлена.  3. Идентификация действительных корней многочлена.  4. Идентификация комплексных корней многочлена. /Лек/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.4 Л1.3Л2.1Л3.1 | |
| 4.2 | Факторизация многочленов над конечным полем и над полем рациональных чисел. /Лаб/ | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | Л1.4 Л1.3Л2.1Л3.1 | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| УП: 44.03.05.29-18-5-МИ.plx | | | |  |  |  |  |  |  |  | стр. 5 |
| 4.3 | | Идентификация действительных и комплексных корней многочлена на основе сортировки. Восстановление коэффициентов. /Лаб/ | | | | 9 | 4 | СК-9 СК-10 СК-11 ПК-7 | | Л1.4 Л1.3Л2.1Л3.1 | |
| 4.4 | | Подготовка реферата / доклада по теме /Ср/ | | | | 9 | 12 | СК-9 СК-10 СК-11 ПК-7 | | Л1.4 Л1.3Л2.1Л3.1 | |
|  | | **Раздел 5. Подготовка к экзамену** | | | |  |  |  | |  | |
| 5.1 | | Подготовка к экзамену /Экзамен/ | | | | 9 | 36 | СК-9 СК-10 СК-11 ПК-7 | | Л1.4 Л1.3 Л1.2 Л1.1Л2.1 Л2.2Л3.1 | |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ** | | | | | | | | | | | |
| Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины. | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ** | | | | | | | | | | | |
| **5.1. Основная литература** | | | | | | | | | | | |
|  | Авторы, составители | | Заглавие | | Издательство, год | | | | Колич-во | | |
| Л1.1 | Голиков А. М. | | Кодирование и шифрование информации в системах связи: курс лекций, компьютерый практикум, задание на самостоятельную работу: учебное пособие | | Томск: ТУСУ�, 2016 | | | | http://biblioclub.ru/index. php? page=book&id=480781 неограниченный доступ для зарегистрированных пользователей | | |
| Л1.2 | Кирьянов, Дмитрий | | Mathcad 15/ Mathcad Prime 1.0 | | СПб.: БХВ-Петербург, 2012 | | | | 15 | | |
| Л1.3 | Шилин, Илья Анатольевич | | Введение в алгебру. Группы: учеб. пособие | | СПб.: Лань, 2012 | | | | 10 | | |
| Л1.4 | Ромм Я.Е., Дордопуло А.И. | | Программная локализация нулей многочленов с приложением к идентификации объектов по данным гидроакустической локации | | Таганрог: Изд-во Таганрог. гос. пед. ин-та, 2005 | | | | 25 | | |
| **5.2. Дополнительная литература** | | | | | | | | | | | |
|  | Авторы, составители | | Заглавие | | Издательство, год | | | | Колич-во | | |
| Л2.1 | Шилин И. А. | | Компьютерная алгебра в задачах: учебное пособие | | Москва: Московский педагогический государственный университет (МПГУ), 2018 | | | | http://biblioclub.ru/index. php? page=book&id=500528 неограниченный доступ для зарегистрированных пользователей | | |
| Л2.2 | Ищейнов В. Я. | | Информационная безопасность и защита информации: теория и практика: учебное пособие | | Москва|Берлин: Директ- Медиа, 2020 | | | | http://biblioclub.ru/index. php? page=book&id=571485 неограниченный доступ для зарегистрированных пользователей | | |
| **5.3. Методические разрабоки** | | | | | | | | | | | |
|  | Авторы, составители | | Заглавие | | Издательство, год | | | | Колич-во | | |
| Л.1 | Ромм, Яков Евсеевич, Тюшнякова, И. А. | | Применение сортировки для поиска нулей и особенностей функций с приложением к идентификации плоских изображений: учеб. пособие для студ. высш. учеб. заведений, обучающихся по спец." Математика и информатика" | | Таганрог: Изд-во Таганрог. гос. пед. ин-та, 2009 | | | | 14 | | |
| **5.3 Профессиональные базы данных и информационные справочные системы** | | | | | | | | | | | |
| **5.4. Перечень программного обеспечения** | | | | | | | | | | | |
| Microsoft Office | | | | | | | | | | | |
| Махima | | | | | | | | | | | |
| DelphiStudio | | | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| УП: 44.03.05.29-18-5-МИ.plx |  | стр. 6 |
| **5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья** | | |
| При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме. | | |
|  |  |  |
| **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | |
| Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет. | | |
|  |  |  |
| **7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | |
| Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины. | | |