федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет
Кафедра математики и методики обучения математике

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Компьютерная алгебра
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Математика. Информатика
Форма обучения: Очная

Разработчики: Тактаров Н. Г., д-р физ.-мат. наук, профессор
Капкаева Л. С., д-р пед. наук, профессор
Ладошкин М. В., канд. физ.-мат. наук, доцент
Дербеденева Н. Н., канд. пед. наук, доцент
Кочетова И. В., канд. пед. наук, доцент
Жаркова Ю. С., канд. физ.-мат. наук, доцент
Базаркина О. А., канд. физ.-мат. наук, доцент
Лапина И. Э., старший преподаватель
Храмова Н. А., ассистент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 12 от 14.06.2018 года

Зав. кафедрой  Ладошкин М. В.
Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 10 от 26.05.2020 года

Зав. кафедрой  Ладошкин М. В.
Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

И. о. зав. кафедрой  Ладошкин М. В.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - овладение основными понятиями и методами абстрактной и компьютерной алгебры, используемыми при реализации образовательных программ по учебным предметам «Алгебра и начала математического анализа», «Информатика и ИКТ» в соответствии с требованиями образовательных стандартов, а также способность осуществлять педагогическое сопровождение социализации и профессионального самоопределения обучающихся.

Задачи дисциплины:

- изучить основные понятия и термины абстрактной и компьютерной алгебры, используемые при реализации образовательных программ по учебным предметам «Алгебра и начала математического анализа», «Информатика и ИКТ» в соответствии с требованиями образовательных стандартов;
- применение методов алгебры и теории чисел для реализации прикладных моделей в криптографии и помехоустойчивом кодировании;
- применение систем символьной математики для реализации образовательных программ по учебным предметам «Алгебра и начала математического анализа», «Информатика и ИКТ» в соответствии с требованиями образовательных стандартов;
- осуществление педагогического сопровождения социализации и профессионального самоопределения обучающихся.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.9 «Компьютерная алгебра» относится к вариативной части учебного плана.

Дисциплина изучается на 3 курсе, в 5 семестре.

Для изучения дисциплины требуется: знание основных понятий курса алгебры и теории чисел.

Изучению дисциплины «Компьютерная алгебра» предшествует освоение дисциплин (практик):

Алгебра.

Освоение дисциплины «Компьютерная алгебра» является необходимой основой для последующего изучения дисциплин (практик):

Защита информации в компьютерных сетях.

Областями профессиональной деятельности бакалавров, на которые ориентирует дисциплина «Компьютерная алгебра», являются образование, социальная сфера, культура.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие;
- просвещение;
- образовательные системы.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-1. готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	
педагогическая деятельность	
ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	знать: - основные задачи теоретической информатики, решаемые методами алгебры и теории чисел; - алгоритмы помехоустойчивого кодирования; - алгоритмы криптографии с открытым ключом; уметь: - реализовывать учебные модели криптографических алгоритмов и модулярной арифметики в программных средах; - применять полиномиальные коды для кодирования и декодирования передаваемой информации; владеть: - алгоритмами помехоустойчивого кодирования; - навыками реализации учебных моделей криптографических алгоритмов и модулярной арифметики в программных средах; - алгоритмами криптографии с закрытым ключом.
ПК-5. способностью осуществлять педагогическое сопровождение социализации и профессионального самоопределения обучающихся	
педагогическая деятельность	
ПК-5 способностью осуществлять педагогическое сопровождение социализации и профессионального самоопределения обучающихся	знать: - основные математические структуры и способы работы с ними; - основные алгоритмические структуры; уметь: - использовать математический аппарат для решения задач; - составлять алгоритмы в системах компьютерной алгебры для решения различных математических задач; владеть: - математикой как универсальным языком науки, средством моделирования явлений и процессов; - навыками составления алгоритмов различного уровня сложности.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Пятый семестр
Контактная работа (всего)	**36**	**36**
Лабораторные	36	36
Самостоятельная работа (всего)	**20**	**20**
Виды промежуточной аттестации		
Экзамен	16	16
Курсовая работа		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1 Содержание модулей дисциплины

Модуль 1. Теория чисел и RSA:

Online математические пакеты. Системы компьютерной алгебры. Алгоритм Евклида. Элементы теории сравнений. Приложения теории сравнений. Афинное кодирование. Системы сравнений. Модулярная арифметика. RSA шифрование.

Модуль 2. Многочлены и помехоустойчивое кодирование:

Разложение на множители. Теория многочленов. Многочлены в системах компьютерной алгебры. Многочлены над конечными полями. Кодирование. Матричное кодирование. Полиномиальное кодирование. Поля Галуа. Код Хемминга.

5.2 Содержание дисциплины: Лабораторные (36 ч.)

Модуль 1. Теория чисел и RSA (18 ч.)

Тема 1. Online математические пакеты (2 ч.)

Online математические программные продукты. Возможности математических и облачных сервисов для организации научной и самостоятельной работы студентов.

Тема 2. Системы компьютерной алгебры (2 ч.)

Visual Basic в Excel. Основные типы данных, операторы. Адресация в Excel.

Тема 3. Алгоритм Евклида (2 ч.)

Расширенный алгоритм Евклида и его табличная и программная реализации. Бинарный алгоритм Евклида.

Тема 4. Элементы теории сравнений (2 ч.)

Применение теории сравнений в простейших задачах криптографии (исторические задачи). Шифр Виженера и его программная реализация.

Тема 5. Приложения теории сравнений (2 ч.)

Реализация некоторых алгоритмов решения сравнений. Таблица Кэли. Программная реализация. Вычисление обратного к обратимому элементу.

Тема 6. Аффинное кодирование (2 ч.)

Аффинное кодирование и декодирование текстовой информации.

Тема 7. Системы сравнений (2 ч.)

Китайская теорема об остатках. Применение теоремы к решению школьных олимпиадных задач.

Тема 8. Модулярная арифметика (2 ч.)

Модулярная арифметика: табличная и программная реализация некоторых алгоритмов модулярной арифметики.

Тема 9. RSA шифрование (2 ч.)

Асимметричные системы. Применение односторонних функций в системах защиты информации.

Модуль 2. Многочлены и помехоустойчивое кодирование (18 ч.)

Тема 10. Разложение на множители (2 ч.)

Основные методы разложения натуральных чисел на множители. Программная реализация одного из методов.

Тема 11. Теория многочленов (2 ч.)

Основные понятия теории многочленов. Нахождение наибольшего общего делителя многочленов.

Тема 12. Многочлены в системах компьютерной алгебры (2 ч.)

Действия с многочленами в системах компьютерной алгебры.

Тема 13. Многочлены над конечными полями (2 ч.)

Многочлены над конечными полями.

Тема 14. Кодирование (2 ч.)

Элементы матричного и группового кодирования.

Тема 15. Матричное кодирование (2 ч.)

Кодирование и декодирование с помощью матриц.

Тема 16. Полиномиальное кодирование (2 ч.)
Кодирование и декодирование с помощью многочленов. Несистематический случай.
Тема 17. Поля Галуа (2 ч.)
Построение полей Галуа.
Тема 18. Код Хемминга (2 ч.)
Практическая реализация кода Хемминга.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1 Вопросы и задания для самостоятельной работы

Пятый семестр (20 ч.)

Модуль 1. Теория чисел и RSA (10 ч.)

Вид СРС: Выполнение индивидуальных заданий
1. Выполнение заданий по вариантам по теме "Теория чисел".
2. Выполнение расшифровки текста по вариантам (аффинное шифрование).

Вид СРС: Подготовка к тестированию
Подготовка к тестированию по модулю "Теория чисел и RSA".

Модуль 2. Многочлены и помехоустойчивое кодирование (10 ч.)

Вид СРС: Выполнение индивидуальных заданий
Выполнение заданий по вариантам по теме "Теория многочленов".

Вид СРС: Подготовка к тестированию
Подготовка к тестированию по модулю "Многочлены и помехоустойчивое кодирование".

Вид СРС: Подготовка к контрольной работе
Подготовка к контрольной работе по модулю "Многочлены и помехоустойчивое кодирование".

7. Тематика курсовых работ (проектов)

1. Многочлены над конечными полями и их применение
2. Системы с открытым ключом
3. Матричное кодирование информации
4. Расширенный алгоритм Евклида и его реализация
5. Факторизация больших натуральных чисел
6. Реализация алгоритмов помехоустойчивого кодирования с помощью многочленов
7. Тестирование больших целых чисел на простоту
8. Аффинное шифрование и его приложения
9. Помехоустойчивое кодирование и его приложения
10. Теория простых чисел и ее приложения

8. Оценочные средства для промежуточной аттестации

8.1 Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ПК-1, ПК-5	3 курс, Пятый семестр	Экзамен Курсовая работа	Модуль 1: Теория чисел и RSA.
ПК-1, ПК-5	3 курс, Пятый семестр	Экзамен Курсовая работа	Модуль 2: Многочлены и помехоустойчивое кодирование.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций: Компетенция ПК-1 формируется в процессе изучения дисциплин:

3D моделирование, Алгебра, Алгоритмический подход в обучении математике, Аналитические вычисления в системах компьютерной математики, Аналитические методы исследования геометрических объектов, Вводный курс математики, Векторно-координатный метод решения геометрических задач, Визуализация и анимация в 3D редакторах, Внеурочная деятельность учащихся по информатике, Воспитательная работа в обучении математике, Вычислительный эксперимент в свободных средах программирования, Геометрические и физические приложения определенного интеграла, Геометрия, Задачи с параметрами и методы их решения, Защита информации в компьютерных сетях, Имитационное моделирование, Интеграция алгебраического и геометрического методов в обучении математике, Интерактивные технологии обучения математике, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Исследовательская и проектная деятельность в обучении математике, Исследовательская и проектная деятельность учащихся по информатике, Исторический подход в обучении математике, Комбинаторные конструкции и производящие функции, Компетентностный подход в обучении математике, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Криптографические основы безопасности, Математические методы обработки экспериментальных данных, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения учащихся нестандартным методам решения математических задач, Методика подготовки к государственной итоговой аттестации по математике, Методология методики обучения математике, Методы аксиоматического построения алгебраических систем, Методы решения задач государственной итоговой аттестации по математике, Методы решения задач по информатике, Методы решения трансцендентных уравнений, неравенств и их систем, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Общая теория линейных операторов и ее приложение к решению геометрических задач, Практикум по информационным технологиям, Применение систем динамической математики в образовании, Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка интерактивного учебного контента, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Реализация прикладной направленности в обучении математике, Решение геометрических задач средствами компьютерного моделирования, Решение задач основного государственного экзамена по математике, Решение задач по криптографии, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение задач повышенного уровня сложности по теории вероятностей, Решение олимпиадных задач по информатике, Решение прикладных задач информатики, Свободное программное обеспечение в образовании, Свободные инструментальные системы, Системы компьютерной математики, Современный урок информатики, Современный урок математики, Теоретические основы информатики, Технологии дополненной и виртуальной реальности, Технологии разработки мобильных приложений, Технологический подход в обучении математике, Технология обучения математическим доказательствам в школе, Технология обучения учащихся решению математических задач, Технология работы с теоремой в обучении математике, Технология разработки и методика проведения элективных курсов по математике, Технология укрупнения дидактических единиц в обучении математике, Формы и методы работы с одаренными детьми, Численные методы, Экстремальные задачи в школьном курсе математики, Элементарная математика, Элементы конструктивной геометрии в школьном курсе математики, Элементы математического анализа в комплексной области, Элементы функционального анализа.

Компетенция ПК-5 формируется в процессе изучения дисциплин:

Вводный курс математики, Интерактивные технологии обучения математике, Информационные системы, Методика обучения информатике, Методика обучения информатике в профильных классах, Методика обучения учащихся нестандартным методам решения математических задач, Методика подготовки к государственной итоговой аттестации по

математике, Методика подготовки учащихся к государственной итоговой аттестации по информатике, Методика решения задач повышенной трудности по информатике, Технология разработки и методика проведения элективных курсов по информатике, Технология разработки и методика проведения элективных курсов по математике, Элементарная математика.

8.2 Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания; умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации		Шкала оценивания по БРС
	Экзамен (дифференцированный зачет)	Зачет	
Повышенный	5 (отлично)	зачтено	90 – 100%
Базовый	4 (хорошо)	зачтено	76 – 89%
Пороговый	3 (удовлетворительно)	зачтено	60 – 75%
Ниже порогового	2 (неудовлетворительно)	незачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Студент демонстрирует знание и понимание основного содержания дисциплины. Владеет методами решения задач по компьютерной алгебре, основными понятиями компьютерной алгебры. Логически верно проводит доказательство теорем. Качественно проводит сравнительный анализ понятий и алгоритмов, дает полные ответы на дополнительные вопросы. Ответ логичен и последователен, отличается глубиной и полнотой раскрытия темы, выводы доказательны.

Хорошо	Студент демонстрирует знание и понимание основного содержания дисциплины. Владеет методами решения задач по компьютерной алгебре, основными понятиями компьютерной алгебры. Доказывает теоремы. Возможно проявление затруднений при сравнительном анализе понятий и алгоритмов, а также при ответе на дополнительные вопросы.
Удовлетворительно	Студент имеет представления о содержании материала, знает и умеет применять основные алгоритмы компьютерной алгебры. Проявляет затруднения при доказательстве утверждений и теорем курса. Допускается несколько ошибок в содержании ответа, при этом ответ отличается недостаточной глубиной и полнотой раскрытия темы.
Неудовлетворительно	Студент демонстрирует незнание основного содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении предлагаемых заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.

8.3 Вопросы, задания текущего контроля

Модуль 1: Теория чисел и RSA

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Опишите расширенный алгоритм Евклида и его использование в школьном курсе математики

2. Опишите способы решения сравнений и их использование в школьном курсе математики

3. Опишите алгоритм симметричного кодирования и его использование в школьном курсе информатики

4. Опишите алгоритм шифрования с открытым ключом и его использование в школьном курсе информатики

ПК-5 способностью осуществлять педагогическое сопровождение социализации и профессионального самоопределения обучающихся

1. Опишите основные приложения теории чисел и их использование в школьном курсе математики

2. Опишите основные методы аффинного шифрования и его использование в школьном курсе математики

Модуль 2: Многочлены и помехоустойчивое кодирование

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Опишите операции над многочленами и их реализацию в системах компьютерной математики

2. Опишите алгоритмы помехоустойчивого кодирования

ПК-5 способностью осуществлять педагогическое сопровождение социализации и профессионального самоопределения обучающихся

1. Опишите приложения теории многочленов над конечными полями в помехоустойчивом кодировании

2. Опишите методы матричного исчисления для решения задач помехоустойчивого кодирования

3. Опишите темы школьного курса математики, использующие теорию многочленов

8.4 Вопросы промежуточной аттестации

Пятый семестр (Экзамен, ПК-1, ПК-5)

1. Опишите расширенный алгоритм Евклида и его реализацию. Рассмотрите применение в

школьном курсе математики и информатики.

2. Сформулируйте алгоритм Евклида, докажите основные свойства. Рассмотрите применение в школьном курсе математики и информатики.

3. Опишите бинарный алгоритм Евклида и выполните его программную реализацию. Рассмотрите применение в школьном курсе математики и информатики.

4. Сформулируйте основные определения: расширенный и бинарный алгоритмы Евклида. Рассмотрите применение в школьном курсе математики и информатики.

5. Опишите шифр Цезаря и аффинное кодирование. Рассмотрите применение в школьном курсе математики и информатики.

6. Сформулируйте понятие аффинного шифрования. Вывод правил зашифровки и расшифровки. Рассмотрите применение в школьном курсе математики и информатики.

7. Сформулируйте теорему Эйлера и малую теорему Ферма. Приведите пример использования этих теорем для решения сравнений. Рассмотрите применение в школьном курсе математики и информатики.

8. Опишите различные случаи решения сравнений. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

9. Охарактеризуйте задачи кодирования с открытым ключом. Опишите конструкцию алгоритма Эль-Гамаля. Рассмотрите применение в школьном курсе математики и информатики.

10. Сформулируйте понятие криптосистемы с открытым ключом. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

11. Охарактеризуйте задачи кодирования с открытым ключом. Опишите конструкцию алгоритма RSA. Проиллюстрируйте на примере. Рассмотрите применение в школьном курсе математики и информатики.

12. Сформулируйте понятие RSA шифрования. Продемонстрируйте на примере работу этой криптосистемы. Рассмотрите применение в школьном курсе математики и информатики.

13. Опишите модулярное представление чисел. Охарактеризуйте действия над числами в модулярном представлении. Рассмотрите применение в школьном курсе математики и информатики.

14. Сформулируйте понятие модулярной арифметики. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

15. Опишите арифметические операции в модулярной арифметике. Восстановление целых чисел по остаткам. Рассмотрите применение в школьном курсе математики и информатики.

16. Сформулируйте понятие криптосистемы с закрытым ключом. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

17. Опишите модулярную арифметику с рациональными числами. Восстановление рационального числа. Рассмотрите применение в школьном курсе математики и информатики.

18. Сформулируйте понятие НОД и НОК чисел. Основные свойства нахождения НОД чисел. Рассмотрите применение в школьном курсе математики и информатики.

19. Сформулируйте вероятностный алгоритм определения простоты числа. Опишите тест Ферма и Миллера-Рабина. Рассмотрите применение в школьном курсе математики и информатики.

20. Опишите вероятностный алгоритм определения простоты чисел. Тестирование на простоту. Рассмотрите применение в школьном курсе математики и информатики.

21. Опишите деление на двучлен и схему Горнера. Объясните, как при помощи схемы Горнера найти корни многочлена. Сформулируйте теорему Безу. Рассмотрите применение в школьном курсе математики и информатики.

22. Сформулируйте понятие схемы Горнера. Продемонстрируйте на примере. Рассмотрите применение в школьном курсе математики и информатики.

23. Дайте определение неприводимых многочленов. Опишите НОД и НОК многочленов. Сформулируйте основную теорему алгебры. Рассмотрите применение в школьном курсе математики и информатики.

24. Сформулируйте понятие неприводимого многочлена. Алгоритмы нахождения НОД и

НОК многочленов. Рассмотрите применение в школьном курсе математики и информатики.

25. Сформулируйте алгоритм деления с остатком в кольце многочленов. Опишите схему Яковкина. Рассмотрите применение в школьном курсе математики и информатики.

26. Сформулируйте понятие схемы Яковкина. Продемонстрируйте на примере. Рассмотрите применение в школьном курсе математики и информатики.

27. Сформулируйте определение конечного поля и его характеристики. Опишите построение поля Галуа. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

28. Опишите понятие конечного поля, его свойства. Продемонстрируйте примеры построения поля Галуа. Рассмотрите применение в школьном курсе математики и информатики.

29. Опишите, как проводится помехоустойчивое кодирование с помощью многочленов. Закодируйте информационное сообщение, допустите ошибку, исправьте ее и декодируйте. Рассмотрите применение в школьном курсе математики и информатики.

30. Сформулируйте понятие помехоустойчивого кодирования. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

31. Опишите построение кода Хэмминга. На примере кода (15,11) закодируйте информационное сообщение, допустите ошибку, исправьте ее и декодируйте. Рассмотрите применение в школьном курсе математики и информатики.

32. Сформулируйте понятие кода Хэмминга. Продемонстрируйте примеры. Рассмотрите применение в школьном курсе математики и информатики.

33. Опишите конструкцию помехоустойчивого кодирования с помощью аппарата теории матриц. Постройте кодирующую и проверочную матрицу. Рассмотрите применение в школьном курсе математики и информатики.

34. Сформулируйте понятие кодирующей и проверочной матриц. Продемонстрируйте на примере их построение. Рассмотрите применение в школьном курсе математики и информатики.

35. Опишите алгебраические и трансцендентные расширения поля. Сформулируйте алгоритм построения расширения поля. Опишите построение поля Галуа. Рассмотрите применение в школьном курсе математики и информатики.

36. Сформулируйте понятие расширения поля. Приведите примеры полей Галуа. Рассмотрите применение в школьном курсе математики и информатики.

37. Приведите пример систематического и несистематического построения помехоустойчивого кода. Рассмотрите применение в школьном курсе математики и информатики.

38. Сформулируйте понятие помехоустойчивого кода. Систематическое и несистематическое построение. Рассмотрите применение в школьном курсе математики и информатики.

39. Опишите алгоритм RSA. Продемонстрируйте его на примере. Рассмотрите применение в школьном курсе математики и информатики.

40. Продемонстрируйте на примерах RSA шифрование. Рассмотрите применение в школьном курсе математики и информатики.

41. Опишите классические схемы шифрования. Продемонстрируйте понятие односторонних функций. Рассмотрите применение в школьном курсе математики и информатики.

42. Сформулируйте понятие односторонних функций. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

43. Опишите варианты метода Гаусса над полем рациональных чисел и над кольцом целых чисел. Рассмотрите применение в школьном курсе математики и информатики.

44. Сформулируйте и докажите метод Гаусса на различными множествами. Продемонстрируйте на примерах. Рассмотрите применение в школьном курсе математики и информатики.

45. Опишите основные понятия теории сравнений. Продемонстрируйте решение сравнений на примерах. Рассмотрите применение в школьном курсе математики и информатики.

46. Опишите понятие сравнения первой степени. Покажите практическое применение теории сравнений в криптографии. Рассмотрите применение в школьном курсе математики и

информатики.

47. Дайте определение системы сравнений. Продемонстрируйте на примерах решение системы сравнений. Рассмотрите применение в школьном курсе математики и информатики.

48. Сформулируйте определение системы сравнений. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

49. Опишите схему Горнера и схему Яковкина. Продемонстрируйте эти алгоритмы на примерах. Рассмотрите применение в школьном курсе математики и информатики.

50. Сформулируйте понятие матричного кодирования. Приведите примеры. Рассмотрите применение в школьном курсе математики и информатики.

8.5 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме экзамена и защиты курсовых работ.

Экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Устный ответ на экзамене

При определении уровня достижений студентов на экзамене необходимо обращать особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– теоретические постулаты подтверждаются примерами из практики.

Тесты

При определении уровня достижений студентов с помощью тестового контроля необходимо обращать особое внимание на следующее:

– оценивается полностью правильный ответ;

– преподавателем должна быть определена максимальная оценка за тест, включающий определенное количество вопросов;

– преподавателем может быть определена максимальная оценка за один вопрос теста;

– по вопросам, предусматривающим множественный выбор правильных ответов, оценка определяется исходя из максимальной оценки за один вопрос теста.

Письменная контрольная работа

Виды контрольных работ: аудиторные, домашние, текущие, экзаменационные, письменные, графические, практические, фронтальные, индивидуальные.

Система заданий письменных контрольных работ должна:

– выявлять знания студентов по определенной дисциплине (разделу дисциплины);

– выявлять понимание сущности изучаемых предметов и явлений, их закономерностей;

– выявлять умение самостоятельно делать выводы и обобщения;

– творчески использовать знания и навыки.

Требования к контрольной работе по тематическому содержанию соответствуют устному

ответу.

Также контрольные работы могут включать перечень практических заданий.

Курсовая работа

При определении уровня достижений студентов по проекту необходимо обращать особое внимание на следующие моменты:

– наличие авторской позиции, самостоятельность суждений;

– соответствие структуры предъявляемым требованиям;

– соответствие содержания теме и структуре работы (проекта);

– полнота и глубина раскрытия основных понятий проблемы;

– использование основной литературы по проблеме;

– теоретическое обоснование актуальности темы и анализ передового опыта работы;

– применение научных методик и передового опыта в своей работе, обобщение собственного опыта, иллюстрируемого различными наглядными материалами, наличие выводов и практических рекомендаций;

– оформление работы (орфография, стиль, цитаты, ссылки и т.д.);

– выполнение работы в срок.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Зюзьков, В. М. Начала компьютерной алгебры [Электронный ресурс] : учеб. пособие / В. М. Зюзьков. – Томск : ТГУ, 2015. – 128 с. – URL : http://biblioclub.ru/index.php?page=book_red&id=480935&sr=1

2. Судоплатов, С. В. Дискретная математика [Электронный ресурс] : учебник / С. В. Судоплатов, Е. В. Овчинникова. - Новосибирск : НГТУ, 2012. - 278 с. - URL : http://biblioclub.ru/index.php?page=book_red&id=135675&sr=1

3. Царев, А. В. Элементы абстрактной и компьютерной алгебры [Электронный ресурс] : учебное пособие / А.В. Царев, Г.В. Шеина. - М. : МПГУ, 2016. - 116 с. - URL : http://biblioclub.ru/index.php?page=book_red&id=471787&sr=1

Дополнительная литература

1. Котова, Л.В. Сборник задач по дисциплине «Методы и средства защиты информации» / Л.В. Котова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский педагогический государственный университет». – Москва : МПГУ, 2015. – 44 с. : – URL: http://biblioclub.ru/index.php?page=book&id=469877

2. Михалева, М.М. Алгебра и теория чисел : учебное пособие / М.М. Михалева, Б.М. Веретенников ; Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2014. – Ч. 1. – 51 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276012

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://mathprofi.ru - Высшая математика для заочников и не только.

2. http://www.allmath.ru/mathan.htm - Вся математика в одном месте. Это математический портал, на котором можно найти любой материал по математическим дисциплинам. Здесь представлены школьная, высшая, прикладная, олимпиадная математика.

3. http://eqworld.ipmnet.ru/ - « Мир математических уравнений» – учебно-образовательная физико-математическая библиотека

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;
– конкретизировать для себя план изучения материала;
– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:
– проработайте каждую тему по предлагаемому ниже алгоритму действий;
– регулярно выполняйте задания для самостоятельной работы, своевременно отчитывайтесь преподавателю об их выполнении;
– изучив весь материал, проверьте свой уровень усвоения содержания дисциплины и готовность к сдаче зачета/экзамена, выполнив задания и ответив самостоятельно на примерные вопросы для промежуточной аттестации.

Алгоритм работы над каждой темой:
– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;
– прочитайте дополнительную литературу из списка, предложенного преподавателем;
– выпишите в тетрадь основные понятия и категории по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к промежуточной аттестации;
– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на аудиторном занятии;
– повторите определения терминов, относящихся к теме;
– продумайте примеры и иллюстрации к обсуждению вопросов по изучаемой теме;
– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;
– продумывайте высказывания по темам, предложенным к аудиторным занятиям.

Рекомендации по работе с литературой:
– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;
– составьте собственные аннотации к другим источникам, что поможет при подготовке рефератов, текстов речей, при подготовке к промежуточной аттестации;
– выберите те источники, которые наиболее подходят для изучения конкретной темы;
– проработайте содержание источника, сформулируйте собственную точку зрения на проблему с опорой на полученную информацию.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1 Перечень программного обеспечения

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010
3. 1С: Университет ПРОФ

12.2 Перечень информационных справочных систем

1. Информационно-правовая система «ГАРАНТ» (http://www.garant.ru)
2. Справочная правовая система «Консультант Плюс» (http://www.consultant.ru)

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata/)
2. Электронная библиотечная система Znanium.com(http://znanium.com/)
3. Единое окно доступа к образовательным ресурсам (http://window.edu.ru

13. Материально-техническое обеспечение дисциплины (модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, № 212.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 11 шт.).

Учебно-наглядные пособия:

Презентации.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), № 108.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы, №225.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации, электронные диски с учебными и учебно-методическими пособиями.