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: Информатика. Математика
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
Базаркина О. А., канд. физ.-мат. наук, доцент
Лапина И. Э., старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 11 от 17.05.2018 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

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 построении различных алгебраических понятий и конструкций, которые имеют приложения в информатике, теории защиты информации, символьных вычислениях.

Задачи дисциплины:

- изучить основные понятия и термины абстрактной и компьютерной алгебры;
- научиться применять методы алгебры и теории чисел для построения некоторых прикладных моделей в криптографии и помехоустойчивом кодировании;
- научиться применять системы символьной математики для решения математических задач.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.09 «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	**16**	**16**
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 (36 ч.)

Модуль 1. Теория чисел и RSA (18 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 (2 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-5	3 курс, Пятый семестр	Экзамен Курсовая работа	Модуль 1: Теория чисел и RSA.
ПК-1	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 и теория чисел, Аналитические вычисления в системах компьютерной математики, Аналитические методы исследования геометрических объектов, Вводный курс математики, 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, Инновационные технологии обучения информатике, Интеграция алгебраического и геометрического методов в обучении математике, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Исследовательская и проектная деятельность учащихся по

информатике, Исторический подход в обучении математике, Комбинаторные конструкции и производящие функции, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Криптографические основы безопасности, Математические методы обработки экспериментальных данных, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения информатике в профильных классах, Методика обучения математике, Методика обучения решению текстовых задач в школьном курсе математики, Методика обучения учащихся нестандартным методам решения математических задач, Методика подготовки и проведения элективных курсов по математике, Методика подготовки учащихся к государственной итоговой аттестации по информатике, Методика решения геометрических задач векторно-координатным методом, Методика решения задач повышенной трудности по информатике, Методы аксиоматического построения алгебраических систем, Методы решения задач государственной итоговой аттестации по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Общая теория линейных операторов и ее приложение к решению геометрических задач, Организация исследовательской и проектной деятельности учащихся по математике, Организация контроля знаний и умений в обучении математике, 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 по криптографии, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение задач повышенного уровня сложности по математическому анализу, 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, Современные средства оценивания результатов обучения, Современный урок информатики, Современный урок математики, Теоретические основы информатики, Теория рядов и ее приложения, Технологии дополненной и виртуальной реальности, Технологии разработки мобильных приложений, Технология обучения математическим доказательствам в школе, Технология обучения математическим понятиям в школе, Технология обучения учащихся решению математических задач, Технология работы с теоремой в обучении математике, Технология разработки и методика проведения элективных курсов по информатике, Технология укрупнения дидактических единиц в обучении математике, 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, Визуализация решений математических задач, Информационные системы, Информационные технологии в научных исследованиях, Компьютерная обработка результатов научного исследования, Методика обучения информатике, Подготовка учебных и научных документов в LaTeX, 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)	
Повышенный	5 (отлично)	90 – 100%
Базовый	4 (хорошо)	76 – 89%
Пороговый	3 (удовлетворительно)	60 – 75%
Ниже порогового	2 (неудовлетворительно)	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Хорошо	Студент демонстрирует знание и понимание основного содержания дисциплины. Экзаменуемый демонстрирует владение основными методами и приемами, изученными в отчетный период. Уверенно отвечает на дополнительные вопросы.
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.
Удовлетворительно	Студент имеет представления о содержании изучаемой дисциплины, владеет основными понятиями и теоремами, изучаемыми в курсе. Применяет основные алгоритмы, затрудняясь в обосновании выбора и возможно допуская негрубые ошибки. Допускается несколько ошибок в содержании ответа, при этом ответ отличается недостаточной глубиной и полнотой раскрытия темы.
Отлично	Студент знает: основные процессы изучаемой предметной области; вычислительные приемы и методы. Экзаменуемый демонстрирует владение всеми вычислительными алгоритмами, может объяснить выбор алгоритма, изменяет путь решения при изменении условия задачи. Полностью и подробно отвечает на дополнительные вопросы

	Ответ логичен и последователен, отличается глубиной и полнотой раскрытия темы, выводы доказательны.

8.3 Вопросы, задания текущего контроля

Модуль 1: Теория чисел и RSA

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

1. Сформулируйте теорему Эйлера и на ее основе обоснуйте алгоритм RSA.
2. Сформулируйте теорему Ферма и на ее основе обоснуйте вероятностный алгоритм разложения на множители.
3. Сформулируйте Китайскую теорему об остатках и на ее основе опишите алгоритм восстановления позиционного представления чисел в модулярной арифметике.
4. Приведите пример афинного кодирования и декодирования информации.

Модуль 2: Многочлены и помехоустойчивое кодирование

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

1. Опишите действия над многочленами. Какие команды в системах компьютерной математики позволяют выполнять действия над многочленами?
2. Опишите неприводимые многочлены над полем комплексных чисел, полем действительных чисел, полем рациональных чисел.
3. Опишите действия с многочленами над конечными полями.
4. Опишите построение кода Хемминга.
5. Опишите построение БЧХ-кода.

8.4 Вопросы промежуточной аттестации

Пятый семестр (Экзамен, ПК-1, ПК-5)

1. Опишите расширенный алгоритм Евклида и его реализацию.
2. Опишите бинарный алгоритм Евклида и выполните его программную реализацию.
3. Опишите шифр Цезаря и аффинное кодирование.
4. Сформулируйте теорему Эйлера и малую теорему Ферма. Приведите пример использования этих теорем для решения сравнений.
5. Охарактеризуйте задачи кодирования с открытым ключом. Опишите конструкцию алгоритма Эль-Гамаля.
6. Охарактеризуйте задачи кодирования с открытым ключом. Опишите конструкцию алгоритма RSA. Проиллюстрируйте на примере.
7. Опишите модулярное представление чисел. Охарактеризуйте действия над числами в модулярном представлении.
8. Опишите арифметические операции в модулярной арифметике. Восстановление целых чисел по остаткам.
9. Опишите модулярную арифметику с рациональными числами. Восстановление рационального числа.
10. Сформулируйте вероятностный алгоритм определения простоты числа. Опишите тест Ферма и Миллера-Рабина.
11. Опишите деление на двучлен и схему Горнера. Объясните, как при помощи схемы Горнера найти корни многочлена. Сформулируйте теорему Безу.
12. Дайте определение неприводимых многочленов. Опишите НОД и НОК многочленов. Сформулируйте основную теорему алгебры.
13. Сформулируйте алгоритм деления с остатком в кольце многочленов. Опишите схему Яковкина.

14. Сформулируйте определение конечного поля и его характеристики. Опишите построение поля Галуа. Приведите примеры.

15. Опишите, как проводится помехоустойчивое кодирование с помощью многочленов. Закодируйте информационное сообщение, допустите ошибку, исправьте ее и декодируйте.

16. Опишите построение кода Хэмминга. На примере кода (15,11) закодируйте информационное сообщение, допустите ошибку, исправьте ее и декодируйте.

17. Опишите конструкцию помехоустойчивого кодирования с помощью аппарата теории матриц. Постройте кодирующую и проверочную матрицу.

18. Опишите алгебраические и трансцендентные расширения поля. Сформулируйте алгоритм построения расширения поля. Опишите построение поля Галуа.

19. Приведите пример систематического и несистематического построения помехоустойчивого кода.

20. Опишите алгоритм RSA. Продемонстрируйте его на примере.

21. Опишите классические схемы шифрования. Продемонстрируйте понятие односторонних функций.

22. Опишите варианты метода Гаусса над полем рациональных чисел и над кольцом целых чисел.

23. Опишите основные понятия теории сравнений. Продемонстрируйте решение сравнений на примерах.

24. Дайте определение системы сравнений. Продемонстрируйте на примерах решение системы сравнений.

25. Опишите схему Горнера и схему Яковкина. Продемонстрируйте эти алгоритмы на примерах.

26. Объясните, как проводить аналитические вычисления с помощью компьютера. Охарактеризуйте системы символьной математики. Приведите примеры. Опишите on-line сервисы символьных вычислений.

27. Сформулируйте понятие бинарного отношения. Приведите примеры. Охарактеризуйте отношение эквивалентности и его свойства, фактор-множество. Приведите примеры.

28. Дайте определение алгебраической структуры. Охарактеризуйте виды алгебр. Опишите свойства бинарных операций. Гомоморфизм и изоморфизм алгебраических структур. Проиллюстрируйте примерами.

29. Дайте определение группы. Сформулируйте их свойства. Опишите таблицу Кэли. Приведите примеры.

30. Дайте определение группы перестановок (симметрическая группа). Опишите решение уравнений в группе перестановок. Приведите примеры применения групп перестановок в криптографии.

31. Дайте определение числовым группам. Приведите примеры. Сформулируйте их свойства.

32. Охарактеризуйте гомоморфизм и изоморфизм групп. Приведите примеры.

33. Охарактеризуйте гомоморфизм групп. Дайте определение ядра гомоморфизма. Сформулируйте теорему о гомоморфизме. Приведите примеры. Дайте определение нормальных подгрупп. Охарактеризуйте факторгруппу.

34. Сформулируйте определение кольца и его свойства. Приведите примеры числовых и функциональных колец.

35. Опишите кольцо целых чисел и его свойства.

36. Охарактеризуйте делители нуля в кольце. Приведите примеры. Дайте определение обратимым элементам кольца. Охарактеризуйте группу обратимых элементов кольца классов вычетов и ее порядок.

37. Сформулируйте определение алгебраической структуры поля. Приведите примеры числовых полей.

38. Охарактеризуйте кольцо классов вычетов и его конструкции. Опишите умножение и деление в кольце классов вычетов.

39. Опишите деление с остатком и алгоритм Евклида в кольце целых чисел. Сформулируйте теорему Ламе.

40. Опишите расширенный алгоритм Евклида и его реализацию.

41. Дайте определение сравнения в кольце целых чисел и сформулируйте их свойства. Опишите решение линейных уравнений в кольце целых чисел.

42. Дайте определения НОД и НОК натуральных чисел. Опишите линейное разложение НОД (алгоритм вычисления).

43. Дайте определение взаимно простых и простых чисел. Сформулируйте алгоритм нахождения простых чисел. Опишите решето Эратосфена.

44. Сформулируйте теорему Эйлера и малую теорему Ферма. Приведите пример использования для решения сравнений.

45. Сформулируйте Китайскую теорему об остатках. Проиллюстрируйте на примере различные методы решения системы линейных сравнений по различным модулям.

46. Опишите модулярное представление чисел. Охарактеризуйте действия над числами в модулярном представлении.

47. Опишите смешанную систему исчисления и ее связь с модулярным представлением.

48. Опишите методы разложения числа на простые множители. Подробно охарактеризуйте метод Ферма.

49. Дайте определение псевдопростым числам. Опишите числа Кармайкла.

50. Сформулируйте вероятностный алгоритм определения простоты числа. Опишите тест Ферма и Миллера-Рабина.

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 позволяет оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные 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.

Собеседование (устный ответ) на экзамене.

Для оценки сформированности компетенции посредством собеседования (устного ответа) студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по изучаемой проблеме;

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

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. Математическая логика и теория алгоритмов : учебное пособие / В.М. Зюзьков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2015. – 236 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480935.

2. 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.

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, курсового проектирования (выполнения курсовых работ).

Лаборатория вычислительной техники.

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).

Лаборатория вычислительной техники.

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 – 14 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал.

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 (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература.

Стенды с тематическими выставками.