МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____ В.Г. Шубаева
«24» мая 2023 г.

# *Дискретная математика*

# Рабочая программа дисциплины

| | |
|---|---|
| Направление подготовки/ *Специальность* | *09.03.03 Прикладная информатика* |
| Направленность (профиль) программы/ *Специализация* | *Управление бизнес-процессами и проектами* |
| Уровень высшего образования | *Бакалавриат* |
| Форма обучения | *очная* |
| Год набора | *2023* |

Составитель*(и)*:

к.физмат.н, Десницкая Валентина Николаевна
к.физмат.н, Дмитриев Владимир Георгиевич

| | | |
|---|---|---|
| Часов по учебному плану | 144 | **Виды контроля в семестрах:** |
| в том числе: | | |
| контактная работа | 48 | Экзамен: семестр 2 |
| самостоятельная работа | 60 | |
| практическая подготовка | 0 | |
| часов на контроль | 36 | |

**Распределение часов дисциплины:**

| Семестр: | 2 |
|---|---|
| Вид занятий | Часы |
| Лекционные занятия | 20 |
| Практические занятия | 28 |
| Лабораторные работы | |
| **Итого аудиторных часов** | **48** |
| Самостоятельная работа | 60 |
| Часы на контроль | 36 |
| **Итого академических часов** | **144** |
| **Общая трудоемкость в зачетных единицах** | **4** |

Санкт-Петербург
2023

# СОДЕРЖАНИЕ

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ** ..... 3

**2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ** ..... 3

**3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ** ..... 3

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*** ..... 4

**5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ** ..... 5

**5.1 Рекомендуемая литература** ..... 5

**5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства** ..... 5

**5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)** ..... 6

**6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ** ..... 6

**7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ** ..... 8

**8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ** ..... 9

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ** ..... 11

**1.1 Контрольные вопросы и задания к промежуточной аттестации** ..... 11

**1.2 Темы письменных работ** ..... 12

**1.3 Контрольные точки** ..... 12

**1.4 Другие объекты оценивания** ..... 13

**1.5 Самостоятельная работа обучающегося** ..... 13

**1.6 Шкала оценивания результата** ..... 13

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

| | |
|---|---|
| **Цель:** | Дать обучающимся необходимый запас сведений по ряду разделов дискретной математики (основные определения, теоремы, правила), наиболее соответствующих их будущей профессиональной деятельности, а также математический аппарат, помогающий им ставить в математической форме и решать профессиональные задачи. |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О Дискретная математика относится к обязательной части Блока 1.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

| **Код и наименование компетенции выпускника** | **Код и наименование индикатора достижения компетенций** | **Планируемые результаты обучения по дисциплине** |
|---|---|---|
| ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | ОПК-3.3 - Анализирует и систематизирует разнородные данные, оценивает эффективность процедур анализа проблем и принятия решений в профессиональной деятельности | Знать: основные положения дискретной математики: элементы теории множеств, элементы теории чисел, теории шифрования.<br>Уметь: использовать математические методы и модели для решения прикладных задач дискретной математики.<br>Владеть: навыками моделирования и решения прикладных задач методами дискретной математики. |
| ОПК-1 - Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности; | ОПК-1.2 - Применяет методы математического анализа для решения стандартных задач в профессиональной деятельности; проводит теоретический анализ и синтез на основе экспериментального исследования при решении стандартных задач в профессиональной деятельности | Знать: основные положения дискретной математики: элементы теории множеств, элементы теории чисел, теории шифрования.<br>Уметь: использовать математические методы и модели для решения прикладных задач дискретной математики.<br>Владеть: навыками моделирования и решения прикладных задач методами дискретной математики. |

# 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

| Номер и наименование тем и/или разделов/тем | Содержание дисциплины | Объем дисциплины (академические часы) | | | |
|---|---|---|---|---|---|
| | | Контактная работа | | | СРО |
| | | ЗЛТ | ПЗ | ЛР | |
| Тема 1. Множества и операции над ними. Отображения, их свойства. Сравнение множеств. | Множества и способы их задания. Числовые множества. Алгебра множеств. Отображения, их свойства. Мощность множества. | 1 | 2 | | 4 |
| Тема 2. Бинарные отношения. Отношения эквивалентности и порядка. | Бинарные отношения, их свойства. Отношение эквивалентности. Классы эквивалентности, фактор-множество. Отношение порядка. Порядок по Парето. Лексикографический порядок. | 2 | 2 | | 4 |
| Тема 3. Делимость чисел. Деление с остатком. Наибольший общий делитель. Алгоритм Евклида. | Делимость чисел, свойства делимости. Деление с остатком. Наибольший общий делитель, его свойства. Вычисление наибольшего общего делителя при помощи алгоритма Евклида. | 2 | 2 | | 6 |
| Тема 4. Решение неопределенных уравнений при помощи алгоритма Евклида. | Взаимно простые числа. Решение неопределенных уравнений при помощи алгоритма Евклида. | 2 | 2 | | 6 |
| Тема 5. Модулярная арифметика. | Сравнения по модулю, их свойства. Нахождение остатков от деления при помощи свойств сравнения по модулю. | 2 | 2 | | 6 |
| Тема 6. Простые числа. Функция Эйлера. Теоремы Эйлера и Ферма. | Простое число. Каноническое разложение числа. Функция Эйлера, ее свойства. Теорема Эйлера, теорема Ферма. Нахождение остатков от деления при помощи теорем Эйлера и Ферма. | 2 | 4 | | 6 |
| Тема 7. Решение сравнений первой степени. Системы сравнений. | Решение сравнений при помощи алгоритма Евклида и при помощи теоремы Эйлера. Системы сравнений. Китайская теорема об остатках. | 3 | 4 | | 8 |
| Тема 8. Цепные дроби. Подходящие дроби, их свойства и применение. | Представление рациональных чисел цепными дробями. Подходящие дроби, их свойства. Решение неопределенных уравнений и сравнений при помощи подходящих дробей. Представление иррациональных чисел цепными дробями. | 2 | 4 | | 8 |

| | | | | | |
|---|---|---|---|---|---|
| Тема 9. Квадратичные вычеты. Проверка чисел на простоту. | Квадратичные вычеты и невычеты. Символ Лежандра, его свойства. Квадратичный закон взаимности Гаусса. Символ Якоби. Алгоритмы проверки чисел на простоту. Вероятностный тест Соловея-Штрассена. | 2 | 4 | | 6 |
| Тема 10. Теория чисел в криптографии. | Задача шифрования. Использование теории чисел в шифровании. Шифр RSA, его обоснование. | 2 | 2 | | 6 |
| **Контроль:** | | | | | **36** |
| **Всего по дисциплине:** | | **20** | **28** | **0** | **60** |

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

# 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

## 5.1 Рекомендуемая литература

| **Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)** | **Электронные ресурсы** |
|---|---|
| Новиков, Ф.А. Дискретная математика: Учебник для вузов. 2-е изд. Стандарт третьего поколения. / Ф.А. Новиков. Санкт-Петербург : Питер, 2021. 432 с. | https://ibooks.ru/bookshelf/377364/reading |
| Судоплатов, С. В. Дискретная математика : учебник и практикум для среднего профессионального образования / С. В. Судоплатов, Е. В. Овчинникова. — 5-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 279 с. | https://urait.ru/viewer/diskretnaya-matematika-445773 |
| Десницкая, Валентина Николаевна. Конспект лекций по дискретной математике : учебное пособие / В.Н. Десницкая, В.Г. Дмитриев, С.В. Петрас ; М-во науки и высш. образования Рос. Федерации, С.-Петерб. гос. экон. ун-т, Каф. высшей математики. Санкт-Петербург, 2019. | http://opac.unecon.ru/elibrary ... B5%D0%BA%D1%86%D0%B8%D0%B9.pdf |
| Вороненко, А. А. Дискретная математика. Задачи и упражнения с решениями: Учебно-методическое пособие / А.А. Вороненко, В.С. Федорова. - Москва : НИЦ ИНФРА-М, 2014. - 104 с. | https://znanium.com/read?id=280162 |

## 5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- ОС Альт образование 10
- LibreOffice

### 5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

| № | Наименование СПБД/ ИСС |
|---|---|
| 1. | Электронная библиотека Grebennikon.ru – www.grebennikon.ru |
| 2. | Научная электронная библиотека eLIBRARRY – www.elibrary.ru |
| 3. | Научная электронная библиотека КиберЛеника – www.cyberleninka.ru |
| 4. | База данных ПОЛПРЕД Справочники – www.polpred.com |
| 5. | База данных OECD Books, Papers & Statistics на платформе OECD iLibrary www.oecd-ilibrary.org |
| 6. | Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru) |
| 7. | Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru) |
| 8. | Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru) |
| 9. | Электронная библиотечная система BOOK.ru - www.book.ru |
| 10. | Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru |
| 11. | Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com |
| 12. | Электронная библиотека СПбГЭУ– opac.unecon.ru |

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

| Наименование учебных аудиторий, перечень | Адрес (местоположение) учебных аудиторий |
|---|---|
| Ауд. 1047 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых | 191023, г. Санкт-Петербург, ул. Канал |

| | |
|---|---|
| работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 42 посадочных мест (парт 21шт.), рабочее место преподавателя, доска меловая 1 шт. (3-х секционная), кафедра 1шт., стул к/з - 2шт. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 2045 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 78 посадочных мест, рабочее место преподавателя, доска меловая (3-х секционная) - 1 шт., кафедра - 1 шт., стульев - 2 шт. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 2067 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 150 посадочных мест, рабочее место преподавателя, доска меловая (4-х секционная) - 1 шт., кафедра - 1 шт., тумба м/м - 1 шт., стол - 1 шт., стул - 3 шт., Компьютер Intel i3-2100 2.4 Ghz/500/4/Acer V193 19" - 1 шт., Мультимедийный проектор Тип 2 Panasonic PT-VX610E - 1 шт., Громкоговоритель 2-полосной Hi-Fi PRO MASKGT-W - 2 шт., Микшер усилитель TA-1120-1 шт. в комплекте с Behringer XM8500 ULTRAVOICE - 1 шт., Экран с электроприводом 183x240 см Компакт - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 2068 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 94 посадочных места, рабочее место преподавателя, доска маркерная - 1 шт., кафедра - 1 шт., стол - 1 шт., стул - 2 шт., Компьютер Intel i3-2100 2.4 Ghz/500/4/Acer V193 19" - 1 шт., Акустическая система JBL CONTROL 25 WH - 2 шт., Экран с электропривод. DRAPER 96 - 1 шт., Акустическая система - 1 шт., Доска магнитно-маркерная 100*200 - 1 шт., Мультимедийный проектор Panasonic PT-VX610E - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |

| | |
|---|---|
| курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | |
| Ауд. 2008 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 60 посадочных мест (стол учебный 30шт., стульев 60шт., рабочее место преподавателя, стол м/м, доска меловая 2 шт.(односекционная), кафедра 1 шт., стул 2шт.Компьютер Intel i3-2100 2.4 Ghz/4/500Gb/Acer V193 19" - 1 шт.,, Мультимедийный проектор Тип 1 Optoma x 400 - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 1043 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 42 посадочных мест (парт 21шт.), рабочее место преподавателя, доска меловая 1 шт. (3-х секционная), кафедра 1шт., стол 2шт., стул изо 2шт.. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |
| Ауд. 0001 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 25 посадочных мест, рабочее место преподавателя, стол 1 шт., доска меловая 1 шт. (2-х секционная), доска маркерная на колесиках 1шт., вешалка стойка 3шт., жалюзи 2шт. Компьютер Intel I5-7400/8Gb/1Tb/ Монитор. DELL S2218H - 24 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия. | 191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р» |

## 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

– учебно-методической документацией;

– локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной

деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
- метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

## 8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

## 1.1 Контрольные вопросы и задания к промежуточной аттестации

1. Множества, операции над множествами, их свойства. Декартово произведение множеств.

2. Отображения. Инъективные, сюръективные и биективные отображения.Функции.

3. Мощность множеств. Равномощные множества. Счетные множества.

4. Множества мощности континуум.

5. Бинарные отношения, их свойства.

6. Отношение эквивалентности, его свойства. Классы эквивалентности, их свойства. Фактор-множество.

7. Отношение порядка.

8. Лексикографический порядок.

9. Порядок по Парето.

10. Графическое изображение бинарных отношений. Таблицы смежности.

11. Делимость чисел. Свойства отношения делимости.

12. Деление с остатком.

13. Наибольший общий делитель чисел, его свойства.

14. Алгоритм Евклида.

15. Линейное представление наибольшего общего делителя.

16. Взаимно простые числа. Необходимое и достаточное условие взаимной

простоты чисел.

17. Сравнение чисел по модулю, его свойства.

18. Простые числа. Каноническое разложение числа на простые

множители.

19. Теорема Евклида о бесконечности множества простых чисел.

20. Функция Эйлера. Теорема о вычислении функции Эйлера. Следствия (свойства функции Эйлера).

21. Теорема Эйлера.

22. Теорема Ферма.

23. Числа, обратные по модулю к данному, их нахождение.

24. Решение сравнений первой степени при помощи алгоритма Евклида.

25. Решение сравнений первой степени при помощи функции Эйлера.

26. Решение неопределенных уравнений при помощи алгоритма Евклида.

27. Решение неопределенных уравнений при помощи функции Эйлера.

28. Системы сравнений.

29. Китайская теорема об остатках.

30. Представление рациональных чисел цепными дробями.

31. Свойства подходящих дробей.

32. Решение неопределенных уравнений при помощи подходящих дробей.

33. Решение сравнений первой степени при помощи подходящих дробей.

34. Представление иррациональных чисел цепными дробями.

35. Квадратичные вычеты и невычеты.

36. Теорема о количестве вычетов и невычетов для простого нечетного числа.

37. Символ Лежандра, его свойства. Решение задачи распознавания при помощи символа Лежандра.

38. Квадратичный закон взаимности Гаусса (без доказательства).

39. Символ Якоби, его свойства. Решение задачи распознавания при помощи символа Якоби.

40. Шифр RSA: описание алгоритма, обоснование алгоритма.

41. Проверка чисел на простоту. Решето Эратосфена.

42. Вероятностный подход к проверке числа на простоту. Тест Соловея-Штрассена

## 1.2 Темы письменных работ

Рабочей программой дисциплины не предусмотрено.

## 1.3 Контрольные точки

| Номер контрольной точки | Тип контрольной точки | Способ проведения | Номера тем |
|---|---|---|---|
| 1 | Контрольное тестирование | письменно | 1-4 |
| 2 | Контрольное тестирование | письменно | 5-9 |
| 3 | Текущий контроль | с помощью технических средств и информационных систем | 1-10 |

## 1.4 Другие объекты оценивания

Рабочей программой дисциплины не предусмотрено.

## 1.5 Самостоятельная работа обучающегося

| Наименования самостоятельной работы | Номера тем |
|---|---|
| Выполнение домашних заданий | 1-10 |
| Подготовка к лекционным и практическим занятиям | 1-10 |
| Подготовка к экзамену | 1-10 |

## 1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.
Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся:**

Формой итогового контроля по дисциплине является экзамен (или дифференцированный зачет), итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

| Баллы | Оценка |
|---|---|
| <=54 | неудовлетворительно |
| 55-69 | удовлетворительно |
| 70-84 | хорошо |
| >=85 | отлично |

**Шкала оценивания результата**

| | |
|---|---|
| 2 (балл до 54) | Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены.<br>Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат. |
| 3 (балл 55-69) | Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены.<br>Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер. |
| 4 (балл 70-84) | Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены.<br>Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения. |

| | |
|---|---|
| 5 (балл 85-100) | Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены.<br>Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход. |