

## АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ «Дискретная математика и теория чисел»

по основной профессиональной образовательной программе по направлению подготовки  
10.03.01 «Информационная безопасность» (уровень бакалавриата)

**Направленность (профиль):** Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)

**Общий объем дисциплины** – 4 з.е. (144 часов)

**Форма промежуточной аттестации** – Экзамен.

**В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:**

- ОПК-3.1: Применяет математический аппарат для решения задач;

**Содержание дисциплины:**

Дисциплина «Дискретная математика и теория чисел» включает в себя следующие разделы:

**Форма обучения очная. Семестр 2.**

**1. Элементы теории множеств, элементы комбинаторики..** Понятие множества, пустое и универсальное множества. Способы задания множеств. Числовые множества. Операции над множествами. Диаграммы Эйлера-Венна. Свойства операций над множествами. Булеан множества и его мощность. Разбиение множества. Декартово произведение множеств и его мощность в случае конечных сомножителей. Бинарные отношения. Конечные бинарные отношения, основные способы задания, представление отношений графами и матрицами. Виды бинарных отношений. Операции над бинарными отношениями, их свойства и выполнение в матричном виде. Основные свойства и матричные признаки специальных конечных однородных бинарных отношений. Замыкания. Матрицы основных замыканий конечного однородного отношения. Отношение эквивалентности и классы эквивалентности. Отношения порядка. Функции. Комбинаторные правила суммы и произведения. Сочетания, размещения, перестановки в схемах выбора с возвращением и без возвращения. Биномиальные коэффициенты и их свойства. Метод включений и исключений. Число функций, биекций, сюръекций..

**2. Булевы функции (функции алгебры логики)..** Понятие булевой функции, основные способы задания. Обзор всех булевых функций одного и двух переменных. Основные законы алгебры логики. Фиктивные и существенные переменные булевой функции. Дизъюнктивные и конъюнктивные нормальные формы булевых функций (ДНФ, КНФ). Совершенные дизъюнктивные и конъюнктивные нормальные формы (СДНФ, СКНФ). Полином Жегалкина. Понятие полноты системы булевых функций. Классы булевых функций. Критерий Поста о полноте. Минимизация булевых функций. Метод карт Карно. Контактные схемы. Функциональные элементы. Схемы из функциональных элементов. Задачи синтеза и анализа..

**3. Элементы теории графов..** Определение графа. Ориентированные, неориентированные и смешанные графы. Изображение графа. Способы задания графов. Полные графы. Двудольные графы. Маршруты в графах. Деревья и их основные свойства. Основные теоремы теории графов. Каркас неориентированного графа, нахождение минимального каркаса неориентированного графа методом Краскала. Алгоритм Дейкстры для нахождения кратчайших маршрутов от одной из вершин до всех остальных вершин графа..

**4. Алгебраические структуры..** Понятие алгебраической операции и алгебраической структуры. Определение и свойства групп. Циклические, симметрические группы. Теорема Кэли. Группа подстановок. Разложение группы по подгруппе. Теорема Лагранжа. Определение и свойства колец. Идеалы, классы вычетов, фактор-кольца. Определение и свойства полей. Поле вычетов. Конечные поля и их свойства..

**5. Основы теории чисел..** Теория делимости. Основные понятия и теоремы. Наибольший общий делитель. Алгоритм Евклида. Наименьшее общее кратное. Простые числа и их свойства. Единственность разложения на простые сомножители. Решето Эратосфена. Непрерывные дроби и их связь с алгоритмом Евклида. Понятие сравнения по данному модулю. Простейшие свойства сравнений. Полная система вычетов по модулю. Функция Эйлера и её основные свойства. Приведенная система вычетов. Теоремы Эйлера и Ферма. Китайская теорема об остатках.

Сравнения первой степени. Система сравнений первой степени. Примеры использования математических методов теории чисел для решения задач профессиональной деятельности..

Разработал:  
доцент  
кафедры ВМ

В.В. Лодейщикова

Проверил:  
Декан ФИТ

А.С. Авдеев