Аннотация рабочей программы дисциплины

Направление подготовки: 02.03.02 «Фундаментальная информатика и информационные технологии»
Тип образовательной программы: академический бакалавриат
Направленность (профиль): Информационная сфера
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

1. **Наименование дисциплины**

Б1.В.ОД.4 Теория чисел и ее приложения

2. **Цели и задачи дисциплины (модуля):**

Целями освоения дисциплины «Теория чисел и ее приложение» являются ознакомление студентов с приемами решения практических задач по теории чисел и шифрованию на открытом ключе, формирование практических умений и навыков, необходимых для приобретения квалификации бакалавр, формирование ключевых профильных компетенций.
Задачи дисциплины – познакомить студентов с теорией чисел, и показать ее приложение к различным областям математики, в том числе в криптографии.

3. **Требования к результатам освоения дисциплины (модуля):**

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

- ОПК-1 – способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и информационными технологиями.
- ПК-1 – способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям
- ПК-2 – способность понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий.

В результате изучения дисциплины студент должен:

Знать: основные теоремы теории чисел и методы решения базовых задач; основные приемы решения задач теории чисел на языке программирования высокого уровня; формулировку задач факторизации и дискретного логарифмирования, методы их решения; основные теоретико-числовые алгоритмы в криптографии.

Уметь: составлять и оформлять программы на языке программирования Java для реализации теоретико-числовых алгоритмов; применять на практике криптографические библиотеки Java; анализировать основные теоретико-числовые алгоритмы в криптографии; применять методы теории чисел в практических задачах.

Владеть: навыками решения задач теории чисел; навыками работы с алгоритмами шифрования на открытом ключе.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры
		6
Аудиторные занятия (всего)	88	88
В том числе:	–	–
Лекции	40	40
Практические занятия (ПЗ)	40	40
Семинары (С)		
Лабораторные работы (ЛР)		
Контроль самостоятельной работы (КСР)	8	8
Самостоятельная работа (всего)	47	47
В том числе:	–	–
Домашние задания	47	47
Вид промежуточной аттестации (зачет, экзамен)		экзамен
Общая трудоемкость часы	180	180
зачетные единицы	5	5

5. Краткая характеристика содержания учебной дисциплины

Раздел 1. Теория делимости
Тема 1.1. Введение в делимость
Тема 1.2. Простые числа
Тема 1.3. Алгоритм Евклида
Тема 1.4. Числовые функции
Тема 1.5. Цепные дроби
Раздел 2. Теория сравнений
Тема 2.1. Введение в сравнения
Тема 2.2. Вычеты по модулю
Тема 2.3. Функция Эйлера
Тема 2.4. Сравнения первой степени
Тема 2.5. Первообразные корни и индексы
Тема 2.6. Сравнения высших степеней
Раздел 3. Шифрование на открытом ключе
Тема 3.1. Асимметричное шифрование
Тема 3.2. Преобразование RSA.
Тема 3.3. Метод ключевого обмена Диффи-Хелмана
Тема 3.4. Преобразование Эль-Гамаля.

6. Форма промежуточной аттестации:

экзамен

7. Разработчик аннотации

доцент кафедры алгебраических и информационных систем, к.ф.-м.н. Л.В. Рябец