АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Теоретико-числовые методы в криптографии»

по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- обеспечение подготовки в одной из важных областей, находящихся на границе теории чисел, информатики и криптографии;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография.

Задачи освоения дисциплины:

- овладение основными вычислительными методами классической и современной теории чисел;
- овладение методами теоретико-числового характера;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография;
- выявление различных приложений теории чисел.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к базовой части цикла Б1 образовательной программы и читается в 6-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов «Вычислительные методы в алгебре и теории чисел», «Информатика», а также некоторых разделов дисциплин «Алгебра и геометрия», «Дискретная математика», «Математическая логика и теория алгоритмов» и «Математический анализ». Кроме того, необходимо наличие практических навыков программирования на одном из языков программирования высокого уровня.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: вычислительные методы в алгебре и теории чисел, элементы высшей алгебры.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Криптографические методы защиты информации», «Криптографические протоколы», «Методы алгебраической геометрии в криптографии», а также для прохождения учебной, производственной и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций.

Код и наименование	Перечень планируемых результатов обучения по

реализуемой компетенции	дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2 – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачетов/экзаменов.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: Лабораторные работы, проверка решения задач.

Промежуточная аттестация проводится в форме: зачет.