АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Теоретико-числовые методы в криптографии»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

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 вариативной части цикла Б1.В (Б1.В.ОД.3) образовательной программы и читается в 6-м семестре студентам специальности «Информационная безопасность автоматизированных систем» 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.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как «Криптографические методы защиты информации», «Криптографические протоколы и стандарты», «Методы алгебраической геометрии в криптографии».

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- 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 (ОПК-2);
- способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1).

В результате изучения дисциплины изучения дисциплины студент должен

Знать:

– основные понятия и методы математического аппарата дисциплины, используемые в криптографии;

– основные теоретико-числовых алгоритмы и особенности их применения;

– оценки эффективности основных теоретико-числовых алгоритмов.

Уметь:

– исследовать и решать сравнения первой и второй степени, системы сравнений по произвольному модулю;

– применять основные теоретико-числовые алгоритмы на практике при решении конкретных задач.

Владеть:

– навыками моделирования и анализа теоретико-числовых алгоритмов;

– навыками эффективного применения основных вычислительных алгоритмов в кольцах вычетов и кольцах многочленов;

– навыками применения аппарата теории чисел в криптографии.

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 зачета.

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: защита лабораторных работ.

Промежуточная аттестация проводится в форме: зачет.