Аннотация к рабочей программе дисциплины

«Теоретико-числовые методы в криптографии»

Курс учебной дисциплины «Теоретико-числовые методы в криптографии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.12.07.

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 академических часа. Учебным планом предусмотрены лекции (36 часов), практические занятия (36 часов), самостоятельная работа студента (72 часа, в том числе 54 часа на подготовку к экзамену). Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теоретико-числовые методы в криптографии» основывается на знаниях, полученных при изучении дисциплин «Математический анализ», «Математическая логика и теория алгоритмов», «Теория вероятностей».

Содержание дисциплины охватывает следующий круг вопросов: оценка сложности арифметических операций, элементы теории чисел, факторизация целых чисел, алгоритмы дискретного логарифмирования, тестирование чисел на простоту

Цель дисциплины – формирование у студентов знаний в области современной алгоритмической теории чисел и ее применении в криптологии.

Задачи дисциплины:

- четкое осознание необходимости и важности математической подготовки для специалиста по компьютерной безопасности;
- ознакомление с основами классической и современной теории чисел, имеющими практические приложения к решению некоторых важных криптографических задач;
- умение давать строгую с математической точки зрения оценку применяемых алгоритмов.

Для успешного изучения дисциплины «Теоретико-числовые методы в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность 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).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) способность 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	Знает	основные понятия математической логики и теории алгоритмов. основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ. основы теории групп и теории групп подстановок. основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности

Для формирования вышеуказанных компетенций в рамках дисциплины «Теоретико-числовые методы в криптографии» применяются следующие

методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).