Аннотация к рабочей программе дисциплины
«Теоретико-числовые методы в криптографии»

Курс учебной дисциплины «Теоретико-числовые методы в криптографии» предназначен для обучения студентов направления 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации» и входит в состав факультативных дисциплин учебного плана ФТД.В.01.

Общая трудоемкость освоения дисциплины составляет 72 часов (2 з.е.). Учебным планом предусмотрены лекционные занятия (18 час.), лабораторные работы (18 час.), самостоятельная работа (36 час.). Дисциплина реализуется на 3 курсе в 5 и 6 семестре. Форма контроля по дисциплине – зачет.

Дисциплина «Теоретико-числовые методы в криптографии» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Теория информации», «Информатика», «Криптографические методы защиты информации».

Содержание дисциплины охватывает следующий круг вопросов: теоретико-числовые алгоритмы в криптографии, криптографические системы и их реализация.

Цель: изложение основ теории чисел и особенностей применения теоретико-числовых алгоритмов при построении криптографических систем.

Задачи:

- изучить основы теории чисел;
- изучить основы теории сложности алгоритмов;
- обозначить перспективы применения результатов теории чисел в криптографической защите информации.

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

- способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-8).

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) Способностью применять соответствующий математический аппарат для решения профессиональных задач	Знает	Применения алгебры высказываний, теории булевых функций, алгебры предикатов, формализованного исчисления.
	Умеет	Использовать законы логики для проверки правильности суждений, решении логических задач, построении доказательств математических утверждений.
	Владеет	Навыками использования логических законов.
(ПК-2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает	модель перевода информации из одной формы в другую и источники ошибок в программном средстве
	Умеет	качественно и концептуально описывать процесс разработки программного средства для конкретной предметной задачи
	Владеет	общей подготовкой (базовыми знаниями) для решения практических задач в предметных областях средствами технологии программирования

Для формирования вышеуказанных компетенций в рамках дисциплины «Теоретико-числовые методы в криптографии» применяются следующие методы обучения: чтение лекций с использованием мультимедийного оборудования (проектор), проведение и сдача лабораторных работ. Используемые оценочные средства: конспект (ПР-7), лабораторные работы (ПР-6).