ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
10.05.03 – Информационная безопасность автоматизированных систем

Аннотация рабочей программы дисциплины «Криптографические методы защиты информации»

Общая трудоемкость дисциплины составляет 6 зач. единиц, 216 часов, форма промежуточной аттестации – экзамен.

Программой дисциплины предусмотрены следующие виды занятий: лекционные – 36 часов, практические – 18 часов, лабораторные – 36 часов, самостоятельная работа обучающегося составляет 126 часов.

Учебным планом предусмотрено выполнение 2 индивидуальных домашних заданий.

Дисциплина подразумевает изучение следующих основных разделов:

Введение в криптографию. Исторический обзор. Открытые сообщения и их характеристики. Критерии распознавания открытого текста.

Основные задачи и понятия криптографии. Перечень угроз. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические проколы.

Основные классы шифров и их свойства. Шифры перестановки. Поточные шифры замены. Шифры гаммирования и их анализ. Анализ шифра Виженера.

Блочные шифры замены. Криптоалгоритмы DES, ГОСТ-28147-98, AES.

Надежность шифров. Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретико-информационный подход к криптографии. Характеристики имитостойкости шифров и их оценки. Помехоустойчивость шифров.

Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Принципы построения криптографических алгоритмов. Типовые генераторы псевдослучайных последовательностей. Генераторы на основе линейных регистров сдвига. Методы анализа криптографических алгоритмов.

Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Алгоритмы шифрования, цифровых подписей, идентификации, распределения ключей.

Хеш-функции и их криптографические приложения. Хеш-функция и аутентификация сообщений. Конструкции MAC на основе симметрического шифрования.