Аннотация дисциплины

Математические основы криптографии

Цель дисциплины:

- формирование основных представлений об использовании криптографических методов, основанных на базе алгебры и теории чисел, для защиты информации при дистанционной передаче электронных финансовых документов, и в платежных системах, использующих электронные деньги.

Место дисциплины в структуре ООП:

- дисциплина по выбору студента математического и естественнонаучного цикла ООП по направлению подготовки 38.03.01 «Экономика», профиль «Бухгалтерский учет, анализ и аудит».

Краткое содержание:

Введение в криптографию. Основные задачи современной криптографии в современных условиях. Математический аппарат, используемый в криптографии. Функция Эйлера и формула ее вычисления. Схема шифрования RSA как пример криптосистемы с открытым ключом. Простые числа. Стойкость криптосистем. Сложность вычислений и односторонние функции в теории чисел. Односторонние функции с секретом. Криптографические протоколы и протокол электронной подписи в криптосистеме RSA. Электронные платежи.