АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ»

Криптографические методы являются весьма распространенными и надежными способами защиты информации. Изучение математических основ криптологии и криптоанализа позволяет решать задачи, на которых базируются современные симметричные и асимметричные криптосистемы, решать задачи элементарного криптоанализа, строить алгоритмы, реализующие генераторы случайных чисел.

В результате изучения дисциплины студент должен:

знать:

- основные виды шифров, математические методы построения шифров;

уметь:

- решать задачи, связанные с математическими операциями, на которых базируются современные симметричные криптосистемы;
- решать задачи, связанные с математическими операциями, на которых базируются современные асимметричные криптосистемы;
- решать задачи элементарного криптоанализа;
- строить алгоритмы, реализующие генераторы случайных чисел;
- пользоваться научно-технической литературой в области математической разработки новых инструментов криптографии;

владеть:

- математической терминологией;
- навыками использования математического аппарата криптографических алгоритмов;
- навыками использования математического аппарата оценки стойкости криптографических алгоритмов.