

АННОТАЦИЯ

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

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
Специализация Безопасность распределённых компьютерных систем
Квалификация выпускника специалист по защите информации
Нормативный период обучения 5 лет и 6 м.
Форма обучения очная
Год начала подготовки 2017

Цель изучения дисциплины: дать будущим инженерам, специализирующимся в области защиты информации, основы знаний о принципах защиты информации с помощью теоретико-числовых методов криптографии.

Задачи изучения дисциплины:

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- дать студентам основы принципов анализа и синтеза шифров;
- ознакомить студентов с математическими методами, используемыми в криптографии;

Перечень формируемых компетенций:

ОПК-2 способностью 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-10 способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах.

ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-10 способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

Общая трудоемкость дисциплины: 2 з.е.

Форма итогового контроля по дисциплине: зачёт.