

АННОТАЦИЯ рабочей программы дисциплины
«Б1.В.ДВ.03.01 Линейные регистры сдвига с обратной связью»

Направление подготовки/специальность 01.04.01 Математика

Объем трудоемкости: 2 зач. ед.

Цель дисциплины:

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

Задачи дисциплины:

Задачи освоения дисциплины «Линейные регистры сдвига с обратной связью»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов, алгоритмов создания псевдослучайных последовательностей. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

Изучение теоретических основ предмета и получение сведений:

об основных задачах и понятиях теории кодирования;

об этапах развития теории кодирования информации;

о классификации псевдослучайных последовательностей;

об алгебраических методах построения псевдослучайных последовательностей;

теории полей Галуа;

неприводимых многочленах над полями Галуа;

характеристических многочленах линейных сдвигов с обратной связью.

Место дисциплины в структуре ООП ВО

Дисциплина «Линейные регистры сдвига с обратной связью» относится к вариативной части блока Б1 Дисциплины и модули и является дисциплиной по выбору

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

Требования к уровню освоения дисциплины: Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-1.

Основные разделы дисциплины:

Линейные рекуррентные последовательности. Свойства периодичности

Регистры сдвига с обратной связью. Производящие функции.

Семейства линейных рекуррентных последовательностей.

Приложения конечных полей Линейные коды Циклические коды. Поточные шифры.

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Автор РПД. д.ф.-м.н., профессор

Рожков А.В.