

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе
«Вероятностно-статистический анализ случайных подстановок»

Ромашко Виктор Романович

Научный руководитель – кандидат физ.-мат. наук, доцент Орлова. Е.Н.

2017

АННОТАЦИЯ

Дипломная работа, 53 страницы, 1 рисунок, 6 таблиц, 6 источников, 1 приложение.

Ключевые слова: ПОДСТАНОВКИ, ЦИКЛОВАЯ СТРУКТУРА, РАВНОВЕРОЯТНАЯ МОДЕЛЬ, СМЕЩЕННЫЕ ПОДСТАНОВКИ, МОДЕЛЬ ЭВАНСА, МОДЕЛИРОВАНИЕ ЦИКЛОВЫХ СТРУКТУР.

Объект исследования — случайные подстановки и их вероятностно-статистические свойства.

Цель работы — исследовать вероятностные свойства цикловой структуры равновероятной модели случайной подстановки, оценить неизвестный параметр неравновероятной модели Эванса.

Методы исследования — методы теории вероятностей и статистического анализа.

В результате исследований вычислены вероятности цикловых структур с заданными свойствами равновероятной модели случайной подстановки. Получены оценки неизвестного параметра неравновероятной модели Эванса.

Областью применения является криптографические системы защиты информации, симуляции, исследование цикловых структур случайных подстановок.

ABSTRACT

Graduate work, 53 pages, 1 figure, 6 tables, 6 sources, 1 supplement.

Keywords: PERMUTATIONS, CYCLE STRUCTUR, EQUIPROBABLE MODEL , DISPLACED PERMUTATIONS, EVANS MODEL, SIMULATION OF CYCLIC STRUCTURES.

The objects of the research are random permutations and their probabilistic-statistical properties.

The goal of the research is investigating the probabilistic properties of the cyclic structure of an equiprobable random substitution model and estimating the unknown parameter of the non-equiprobable Evans model.

The research methods - methods of probability theory and statistical analysis.

In **the result of research** were calculated probabilities of cyclic structures with given properties of an equiprobable random substitution model. Estimates of the unknown parameter of the non-equiprobable Evans model are obtained.

The application area is cryptographic information protection systems, simulations, investigation of the cyclic structures of random substitutions.