

# **ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА**

---

---

*Научный журнал*

---

---

2018

№ 41

Зарегистрирован в Федеральной службе по надзору  
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

**УЧРЕДИТЕЛЬ**  
**Томский государственный университет**

**РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА**  
**«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»**

Агибалов Г. П., д-р техн. наук, проф. (главный редактор); Девянин П. Н., д-р техн. наук, чл.-корр. Академии криптографии РФ (зам. гл. редактора); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. гл. редактора); Панкратова И. А., канд. физ.-мат. наук, доц. (отв. секретарь); Агиевич С. В., канд. физ.-мат. наук; Алексеев В. Б., д-р физ.-мат. наук, проф.; Быкова В. В., д-р физ.-мат. наук, проф.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Колесникова С. И., д-р техн. наук; Крылов П. А., д-р физ.-мат. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Мясников А. Г., д-р физ.-мат. наук, проф.; Романьков В. А., д-р физ.-мат. наук, проф.; Салий В. Н., канд. физ.-мат. наук, проф.; Сафонов К. В., д-р физ.-мат. наук, проф.; Фомичев В. М., д-р физ.-мат. наук, проф.; Харин Ю. С., д-р физ.-мат. наук, чл.-корр. НАН Беларуси; Чеботарев А. Н., д-р техн. наук, проф.; Шоломов Л. А., д-р физ.-мат. наук, проф.

**Адрес редакции и издателя:** 634050, г. Томск, пр. Ленина, 36  
**E-mail:** vestnik\_pdm@mail.tsu.ru

*В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.*

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*  
Верстка *И. А. Панкратовой*

---

Подписано к печати 17.09.2018. Формат 60 × 84<sup>1</sup>/<sub>8</sub>. Усл. п. л. 14,6. Тираж 300 экз.  
Заказ № 3366. Цена свободная. Дата выхода в свет 28.09.2018.

---

Отпечатано на оборудовании  
Издательского Дома Томского государственного университета  
634050, г. Томск, пр. Ленина, 36  
Тел.: 8(3822)53-15-28, 52-98-49

# СОДЕРЖАНИЕ

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Анохин М. И. О числе однородных невырожденных $p$ -ичных функций заданной степени .....	5
Идрисова В. А. О построении APN-перестановок с помощью подфункций .....	17

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Денисов О. В. Критерии марковости алгоритмов блочного шифрования.....	28
Романьков В. А., Обзор А. А. Метод нелинейного разложения для анализа криптографических схем, использующих автоморфизмы групп.....	38

## ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Артемова Н. А. Периоды $\varphi$ -графов .....	46
Белим С. В., Богаченко Н. Ф. Проверка соответствия ориентированного графа алгебраической решётке.....	54
Лебедев Ф. В. Структурные свойства минимальных примитивных орграфов .....	66
Монахова Э. А. Новые семейства мультипликативных циркулянтных сетей .....	76

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рязанов Ю. Д. Минимизация синтаксических диаграмм с многоходовыми компонентами .....	85
--	----

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Гейдаров П. Ш. Архитектура нейронной сети с попарно последовательным разделением образов.....	98
Колосов В. С. Метод последовательной активации ограничений в линейном программировании .....	110
СВЕДЕНИЯ ОБ АВТОРАХ .....	126

# CONTENTS

## THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

<b>Anokhin M. I.</b> On the number of homogeneous nondegenerate $p$ -ary functions of the given degree .....	5
<b>Idrisova V. A.</b> On constructing APN permutations using subfunctions .....	17

## MATHEMATICAL METHODS OF CRYPTOGRAPHY

<b>Denisov O. V.</b> Criteria for Markov block ciphers .....	28
<b>Roman'kov V. A., Obzor A. A.</b> A nonlinear decomposition method in analysis of some encryption schemes using group automorphisms .....	38

## APPLIED GRAPH THEORY

<b>Artemova N. A.</b> Periods of $\varphi$ -graphs .....	46
<b>Belim S. V., Bogachenko N. F.</b> The check of the correspondence of the directed graph to the algebraic lattice .....	54
<b>Lebedev P. V.</b> Structural properties of minimal primitive digraphs .....	66
<b>Monakhova E. A.</b> New families of multiplicative circulant networks .....	76

## MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

<b>Ryazanov Yu. D.</b> Minimization of syntax diagrams with multiport components .....	85
--	----

## COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

<b>Geidarov P. Sh.</b> The architecture of a neural network with a sequential division of images into pairs .....	98
<b>Kolosov V. S.</b> Method for sequential activation of limitations in linear programming .....	110
<b>BRIEF INFORMATION ABOUT THE AUTHORS</b> .....	126