

# **ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА**

---

---

*Научный журнал*

---

---

2018

№ 39

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); Алексеев В. Б., д-р физ.-мат. наук, проф.; Бандман О. Л., д-р техн. 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, доц.; 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 14.03.2018. Формат  $60 \times 84\frac{1}{8}$ . Усл. п. л. 15. Тираж 300 экз.  
Заказ № 3060. Цена свободная. Дата выхода в свет 30.03.2018.

---

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

|   |    |
|---|----|
| Зуев Ю. А. Об экстремальных вероятностях осуществления $k$ из $n$ событий .....     | 5  |
| Шоломов Л. А. Об одном инварианте в задаче разложения недоопределённых данных ..... | 13 |

### МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

|   |    |
|---|----|
| Agievich S. V. ENE: nonce misuse-resistant message authentication ..... | 33 |
|---|----|

### МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

|  |    |
|--|----|
| Гайдамакин Н. А. Многоуровневое тематико-иерархическое управление доступом (MLTHS-система) ..... | 42 |
| Девянин П. Н. Уровень запрещающих ролей иерархического представления МРОСЛ ДП-модели .....       | 58 |

### ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

|   |    |
|---|----|
| Литичевский Д. В. Списочное декодирование биортогональных вейвлет-кодов с заданным кодовым расстоянием в поле нечётной характеристики ..... | 72 |
|---|----|

### ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

|  |    |
|--|----|
| Логачев О. А. О локальной обратимости конечных автоматов без потери информации ..... | 78 |
|--|----|

### МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

|  |    |
|--|----|
| Никитин А. Ю., Рыбалов А. Н. О сложности проблемы разрешимости систем уравнений над конечными частичными порядками ..... | 94 |
| Песняк А. А., Стефанцов Д. А. Интервалы индексов в ЛЯПАСе .....  | 99 |

### ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

|  |     |
|--|-----|
| Бурделев А. В. О сходимости нового алгоритма характеристики $k$ -значных пороговых функций ..... | 107 |
| Дмитриев И. Н. Быстрый алгоритм кластерного анализа $k$ -medoids .....                           | 116 |
| СВЕДЕНИЯ ОБ АВТОРАХ .....  | 128 |

# CONTENTS

## THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

|   |    |
|---|----|
| <b>Zuev Yu. A.</b> On extreme joint probabilities of $k$ events chosen from $n$ events .....    | 5  |
| <b>Sholomov L. A.</b> On an invariant for the problem of underdetermined data decomposing ..... | 13 |

## MATHEMATICAL METHODS OF CRYPTOGRAPHY

|  |    |
|--|----|
| <b>Agievich S. V.</b> EHE: nonce misuse-resistant message authentication ..... | 33 |
|--|----|

## MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

|  |    |
|--|----|
| <b>Gaydamakin N. A.</b> Multilevel thematic-hierarchical access control (MLTHS-system) .....                 | 42 |
| <b>Devyanin P. N.</b> The level of negative roles of the hierarchical representation of MROSL DP-model ..... | 58 |

## APPLIED CODING THEORY

|  |    |
|--|----|
| <b>Litichevskiy D. V.</b> List decoding of the biorthogonal wavelet code with predetermined code distance on a field of odd characteristic ..... | 72 |
|--|----|

## APPLIED THEORY OF AUTOMATA

|  |    |
|--|----|
| <b>Logachev O. A.</b> On the local invertibility of finite state information lossless automata ..... | 78 |
|--|----|

## MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

|   |    |
|---|----|
| <b>Nikitin A. Y., Rybalov A. N.</b> On complexity of the satisfiability problem of systems over finite posets ..... | 94 |
| <b>Pesnyak A. A., Stefantsov D. A.</b> Index intervals in LYaPAS .....  | 99 |

## COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

|  |     |
|--|-----|
| <b>Burdelev A. V.</b> Convergence of an iterative algorithm for computing parameters of multi-valued threshold functions ..... | 107 |
| <b>Dmitriev I. N.</b> Fast algorithm of cluster analysis $k$ -medoids .....  | 116 |
| <b>BRIEF INFORMATION ABOUT THE AUTHORS</b> .....   | 128 |