

РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА  
«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»

Агибалов Г. П., д-р техн. наук, проф. (председатель); Девянин П. Н., д-р техн. наук, доц. (зам. председателя); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. председателя); 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.; Чеботарев А. Н., д-р техн. наук, проф.; Шойтов А. М., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ; Шоломов Л. А., д-р физ.-мат. наук, проф.

**Адрес редакции:** 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 22.12.2015.

Формат 60 × 84 $\frac{1}{8}$ . Усл. п. л. 12,8. Уч.-изд. л. 14,2. Тираж 300 экз. Заказ № 1523.

---

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

Бугров А. Д. Кусочно-аффинные подстановки конечных полей .....	5
Кочергин В. В., Михайлович А. В. О сложности схем в базисах, содержащих монотонные элементы с нулевыми весами .....	24
Тришин А. Е. О показателе нелинейности кусочно-линейных подстановок адди- тивной группы поля $\mathbb{F}_{2^n}$ .....	32

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Медведева Н. В., Титов С. С. Описание неэндоморфных максимальных со- вершенных шифров с двумя шифрвеличинами .....	43
Нестеренко А. Ю., Пугачев А. В. Об одной схеме гибридного шифрования .....	56

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Колегов Д. Н., Брославский О. В., Олексов Н. Е. Исследование возмож- ности управления веб-браузерами на основе фреймворка ВеЕF и облачного сервиса Google Drive .....	72
---	----

## ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

Ширяев П. М. Сравнение кода Голея с алгеброгеометрическим кодом .....	77
---	----

## ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Зубов А. Ю. О некоторых классах экстремальных ориентированных графов .....	83
Комаров Д. Д. Верхняя оценка количества дополнительных рёбер минималь- ных рёберных 1-расширений сверхстройных деревьев .....	91

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Адельшин А. В., Колоколов А. А. Анализ и решение задач дискретной опти- мизации с логическими ограничениями на основе $L$ -разбиения .....	100
---	-----

## ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Дронов С. В., Бойко И. Ю. Метод оценки степени связи бинарного и номи- нального показателей .....	109
СВЕДЕНИЯ ОБ АВТОРАХ .....	120

# CONTENTS

## THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

<b>Bugrov A. D.</b> Piecewise-affine permutations of finite fields .....	5
<b>Kochergin V. V., Mikhailovich A. V.</b> On the complexity of circuits in bases containing monotone elements with zero weights .....	24
<b>Trishin A. E.</b> The nonlinearity index for a piecewise-linear substitution of the ad- ditive group of the field $\mathbb{F}_{2^n}$ .....	32

## MATHEMATICAL METHODS OF CRYPTOGRAPHY

<b>Medvedeva N. V., Titov S. S.</b> Description of non-endomorphic maximum perfect ciphers with two-valued plaintext alphabet .....	43
<b>Nesterenko A. Yu., Pugachev A. V.</b> A new hybrid encryption scheme .....	56

## MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

<b>Kolegov D. N., Broslavsky O. V., Oleksov N. E.</b> Hooked-browser network with BeEF and Google Drive .....	72
--	----

## APPLIED CODING THEORY

<b>Shiriaev P. M.</b> Comparison of the binary Golay code with the algebro-geometric code .....	77
--	----

## APPLIED GRAPH THEORY

<b>Zubov A. Yu.</b> About some classes of extremal oriented graphs .....	83
<b>Komarov D. D.</b> Upper bound for the number of additional edges in minimal 1-edge extensions of starlike trees .....	91

## COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

<b>Adelshin A. V., Kolokolov A. A.</b> Analysis and solution of discrete optimization problems with logical constraints on the base of $L$ -partition approach .....	100
---	-----

## DISCRETE MODELS FOR REAL PROCESSES

<b>Dronov S. V., Boyko I. Yu.</b> Method for estimating connection power of binary and nominal variables .....	109
---	-----

BRIEF INFORMATION ABOUT THE AUTHORS .....	120
---	-----