

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2018

№ 40

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.; 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 14.06.2018. Формат 60 × 84 $\frac{1}{8}$. Усл. п. л. 14,8. Тираж 300 экз.
Заказ № 3239. Цена свободная. Дата выхода в свет 29.06.2018.

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

Сошин Д. А. Класс сбалансированных алгебраических пороговых функций	5
Черемушкин А. В. О линейной разложимости двоичных функций	10

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions	23
Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography	34

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

Монарёв В. А., Пестунов А. И. Эффективное обнаружение стеганографиче- ски скрытой информации посредством интегрального классификатора на ос- нове сжатия данных	59
---	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Шейдаев В. Ф., Гамаюнов Д. Ю. Отказуемые групповые коммуникации в мо- дели глобального неограниченного злоумышленника	72
--	----

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Володичева М. И., Леора С. Н. Исследование изоморфизма графов с помо- щью жордановых форм матриц смежности	87
---	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рыбалов А. Н. Релятивизованные генерические классы P и NP	100
Тарков М. С. Построение сети Хемминга на основе кроссбара с бинарными мемристорами	105

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Мирзабеков Я. М., Шихиев Ш. Б. Формальная грамматика русского языка в примерах	114
СВЕДЕНИЯ ОБ АВТОРАХ	127

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Soshin D. A. The class of balanced algebraic threshold functions	5
Cheremushkin A. V. Linear decomposition of Boolean functions into a sum or a product of components	10

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Agibalov G. P., Pankratova I. A. Asymmetric cryptosystems on Boolean functions	23
Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography	34

MATHEMATICAL METHODS OF STEGANOGRAPHY

Monarev V. A., Pestunov A. I. Efficient steganography detection by means of compression-based integral classifier	59
--	----

MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

Sheidaev V. F., Gamayunov D. Y. Deniable group communications in the presence of global unlimited adversary	72
--	----

APPLIED GRAPH THEORY

Volodicheva M. I., Leora S. N. Study of graph isomorphism using Jordan forms of adjacency matrices	87
---	----

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Rybalov A. N. Relativized generic classes P and NP	100
Tarkov M. S. Construction of a Hamming network based on a crossbar with binary memristors	105

DISCRETE MODELS FOR REAL PROCESSES

Mirzabekov Ya. M., Shihiev Sh. B. Formal grammar of Russian language in examples	114
---	-----

BRIEF INFORMATION ABOUT THE AUTHORS	127
---	-----