

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2016

№ 2(32)

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



ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**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 15.06.2016.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз. Заказ № 1918.

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

Лукьянова Н. А., Семенова Д. В. Ассоциативные функции Франка в построении семейств дискретных вероятностных распределений случайных множеств событий.....	5
Сошин Д. А. Построение подстановок на основе пороговых функций многозначной логики	20

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Денисов О. В., Былина Р. А. Матричная формула для распределения выхода блочной схемы шифрования и статистический критерий на ее основе	33
Зубов А. Ю. Об оценке стойкости AEAD-криптосистемы типа GCM	49
Новоселов С. А. Границы сбалансированной степени вложения для криптографии на билинейных спариваниях	63

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

Монарёв В. А., Пестунов А. И. Повышение эффективности методов стегоанализа при помощи предварительной фильтрации контейнеров	87
--	----

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Курапов С. В., Давидовский М. В. Проверка планарности и построение топологического рисунка плоского графа (поиском в глубину)	100
Салий В. Н. О количестве шпернеровых вершин в дереве.....	115

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рыбалов А. Н. О генерической сложности проблемы общезначимости булевых формул	119
СВЕДЕНИЯ ОБ АВТОРАХ	127

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Lukyanova N. A., Semenova D. V. Associative Frank functions in constructing families of discrete probability distributions of random sets of events	5
Soshin D. A. Constructing substitutions on the basis of threshold functions of multivalued logic	20

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Denisov O. V., Bylina R. A. Matrix formula for the spectrum of output distribution of block cipher scheme and statistical criterion based on this formula	33
Zubov A. Yu. On the security of AEAD-cryptosystem of the GCM type	49
Novoselov S. A. On bounds for balanced embedding degree	63

MATHEMATICAL METHODS OF STEGANOGRAPHY

Monarev V. A., Pestunov A. I. Enhancing steganalysis accuracy via tentative filtering of stego-containers	87
--	----

APPLIED GRAPH THEORY

Kurapov S. V., Davidovsky M. V. Planarity testing and constructing the topological drawing of a plane graph (DFS)	100
Salii V. N. On the number of Sperner vertices in a tree	115

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Rybalov A. N. On generic complexity of the validity problem for Boolean formulas	119
BRIEF INFORMATION ABOUT THE AUTHORS	127