

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2016

№ 3(33)

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 15.09.2016.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз. Заказ № 2085.

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

Ильев А. В., Ильев В. П. Характеризация матроидов в терминах поверхностей.....	5
--	---

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Городилова А. А. От криптоанализа шифра к криптографическому свойству булевой функции	16
Зубов А. Ю. О понятии ε -совершенного шифра	45
Сошин Д. А. Задание подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ с помощью алгебраических пороговых функций	53

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Магомедов А. М. Цепочечные структуры в задачах о расписаниях.....	67
Фомичев В. М. Новая универсальная оценка экспонентов графов	78

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Дурнев В. Г., Зеткина О. В., Зеткина А. И., Мурин Д. М. О coNP-полноте задачи «Инъективный рюкзак»	85
Рыбалов А. Н. О генерической сложности проблемы дискретного логарифма	93
Снытникова Т. В., Непомнящая А. Ш. Решение задач на графах с помощью STAR-машины, реализуемой на графических ускорителях	98

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Кузнецов А. А. Об одном алгоритме вычисления функций роста в конечных двупорождённых группах периода 5	116
СВЕДЕНИЯ ОБ АВТОРАХ	126

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Il'ev A. V., Il'ev V. P. A characterization of matroids in terms of surfaces	5
---	---

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Gorodilova A. A. From cryptanalysis to cryptographic property of a Boolean function	16
Zubov A. U. On the concept of a ε -perfect cipher	45
Soshin D. A. The implementation of Magma and 2-GOST block cipher substitutions by algebraic threshold functions	53

APPLIED GRAPH THEORY

Magomedov A. M. Chain structures in schedules tasks	67
Fomichev V. M. The new universal estimation for exponents of graphs	78

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Durnev V. G., Zetkina O. V., Zetkina A. I., Murin D. M. About the coNP-complete "Injective knapsack" problem	85
Rybalov A. N. On generic complexity of the discrete logarithm problem	93
Snytnikova T. V., Nepomniaschaya A. Sh. Solution of graph problems by means of the STAR-machine being implemented on GPUs	98

COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

Kuznetsov A. A. An algorithm for computation of the growth functions in finite two-generated groups of exponent 5	116
--	-----

BRIEF INFORMATION ABOUT THE AUTHORS	126
--	-----