

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2017

№ 36

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, доц. (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 20.06.2017. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,8. Уч.-изд. л. 16,3.
Тираж 300 экз. Заказ № 2609. Цена свободная. Дата выхода в свет 4.07.2017.

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

Вахрамеев М. А. Случайные уравнения над свободными полурешётками	5
Волгин А. В. Улучшение оценки скорости сходимости в многомерной центральной предельной теореме для сумм локально зависимых случайных векторов	13
Глухов М. М., Камловский О. В. Применение сумм Гаусса для вычисления точных значений числа появлений элементов поля на циклах линейных рекуррентных последовательностей	25
Roman'kov V. A. On solvability of regular equations in the variety of metabelian groups ..	51

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Агибалов Г. П. Криптоавтоматы с функциональными ключами	59
Щуренко А. В., Леонтьев В. Л. Финитные функции в алгоритмах криптографии	73

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Сковорода А. А., Гамаюнов Д. Ю. Анализ мобильных приложений с использованием моделей привилегий и API-вызовов вредоносных приложений	84
--	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рыбалов А. Н. О генерической NP-полноте проблемы выполнимости булевых формул.	106
---	-----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

Быкова В. В., Катаева А. В. О избыточном представлении минимаксного базиса строгих ассоциативных правил	113
СВЕДЕНИЯ ОБ АВТОРАХ	127

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Vakhrameev M. A. Random equations over free semilattices	5
Volgin A. V. Improving the rate of convergence in the multidimensional central limit theorem for sums of locally dependent random vectors	13
Glukhov M. M., Kamlovskii O. V. Application of Gauss sums to calculate the ex- act values of the number of appearances of elements on cycles of linear recurrences	25
Roman'kov V. A. On solvability of regular equations in the variety of metabelian groups	51

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Agibalov G. P. Cryptautomata with functional keys	59
Shchurenko A. V., Leontiev V. L. Compactly supported functions in cryptogra- phy algorithms	73

MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY

Skovoroda A. A., Gamayunov D. Y. Automated static analysis and classification of Android malware using permission and API calls models	84
--	----

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Rybalov A. N. On generic NP-completeness of the Boolean satisfiability problem	106
---	-----

MATHEMATICAL BACKGROUNDS OF INTELLIGENT SYSTEMS

Bykova V. V., Kataeva A. V. On the non-redundant representation of the mini- max basis of strong associations	113
BRIEF INFORMATION ABOUT THE AUTHORS	127