

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2015

№ 3(29)

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, проф.; 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 15.09.2015.

Формат 60 × 84 $\frac{1}{8}$. Усл. п. л. 12,8. Уч.-изд. л. 14,2. Тираж 300 экз. Заказ № 1282.

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

Андреев А. А. О нижних оценках сложности функций многозначной логики над бесконечными базисами.....	5
Биляк И. Б., Камловский О. В. Частотные характеристики циклов выходных последовательностей комбинирующих генераторов над полем из двух элементов	17

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Романьков В. А. Новая семантически стойкая система шифрования с открытым ключом на базе RSA.....	32
Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V. Problems, solutions and experience of the first international student's Olympiad in cryptography	41

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Жаркова А. В. Количество недостижимых состояний в конечных динамических системах двоичных векторов, ассоциированных с ориентациями пальм.....	63
Козин И. В., Курапов С. В., Полюга С. И. Эволюционно-фрагментарный алгоритм нахождения максимального планарного суграфа	74
Назаров М. Н. Об альтернативном способе задания конечных графов	83
Носов Ю. Л. О максимальных внешнеплоских графах с двумя симплициальными вершинами	95

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Витвицкий А. А. Построение неоднородного массива ячеек для задач клеточно-автоматного моделирования роста и деления клеток бактерий.....	110
СВЕДЕНИЯ ОБ АВТОРАХ	121

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Andreev A. A. On lower bounds for complexity over infinite bases for functions of multi-valued logic	5
Bilyak I. B., Kamlovskii O. V. Frequency characteristics of cycles in output sequences generated by combining generators over the field of two elements	17

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Romankov V. A. A semantically secure public-key cryptosystem based on RSA	32
Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V. Problems, solutions and experience of the first international student's Olympiad in cryptography	41

APPLIED GRAPH THEORY

Zharkova A. V. Number of inaccessible states in finite dynamic systems of binary vectors associated with palms orientations	63
Kozin I. V., Kurapov S. V., Poljuga S. I. Evolutionarily-fragmented algorithm for finding a maximal flat part of a graph	74
Nazarov M. N. An alternative way of defining finite graphs	83
Nosov Y. L. Maximal outerplane graphs with two simplicial vertices	95

DISCRETE MODELS FOR REAL PROCESSES

Vitvitsky A. A. Construction of inhomogeneous 3D mesh for simulation of bacterial cell growth and division by cellular automata	110
BRIEF INFORMATION ABOUT THE AUTHORS	121