

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2018

№ 42

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»

Агibalов 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); Агиевич С. В., канд. физ.-мат. наук; 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 17.12.2018. Формат 60 × 84 $\frac{1}{8}$. Усл. п. л. 15,5. Тираж 300 экз.
Заказ № 3583. Цена свободная. Дата выхода в свет 21.12.2018.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

ПАМЯТИ МИХАИЛА МИХАЙЛОВИЧА ГЛУХОВА	5
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ	
Миронкин В. О. Об оценках распределения длины отрезка аperiodичности в графе k -кратной итерации равновероятного случайного отображения	6
Чередник И. В. Один подход к построению кратно транзитивного множества блочных преобразований	18
МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ	
Боровкова И. В., Панкратова И. А., Семенова Е. В. Криптоанализ двух- каскадного конечно-автоматного генератора с функциональным ключом	48
Agibalov G. P. ElGamal cryptosystems on Boolean functions	57
ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ	
Ильев А. В., Ильев В. П. Об одной задаче кластеризации графа с частичным обучением	66
Ключарёв П. Г. Детерминированные методы построения графов Рамануджана, предназначенных для применения в криптографических алгоритмах, основан- ных на обобщённых клеточных автоматах	76
ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ	
Кузнецов А. А., Кузнецова А. С. Ресурсно-эффективный алгоритм для ис- следования роста в конечных двупорождённых группах периода 5	94
ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ	
Газдюк Е. П., Жихаревич В. В., Никитина О. М., Остапов С. Э. Модели- рование движения одноклеточного микроорганизма «Amoeba Proteus» мето- дом подвижных клеточных автоматов	104
МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ	
Нефёдов В. Н., Смерчинская С. О., Яшина Н. П. Построение агрегирован- ного отношения, минимально удалённого от экспертных предпочтений	120
СВЕДЕНИЯ ОБ АВТОРАХ	133

CONTENTS

IN MEMORY OF MIKHAIL MIKHAILOVICH GLUKHOV	5
THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS	
Mironkin V. O. On estimations of distribution of the length of aperiodicity segment in the graph of k -fold iteration of uniform random mapping	6
Cherednik I. V. One approach to constructing a multiply transitive class of block transformations	18
MATHEMATICAL METHODS OF CRYPTOGRAPHY	
Borovkova I. V., Pankratova I. A., Semenova E. V. Cryptanalysis of 2-cascade finite automata generator with functional key	48
Agibalov G. P. ElGamal cryptosystems on Boolean functions	57
APPLIED GRAPH THEORY	
Ilev A. V., Il'ev V. P. On a semi-superwized graph clustering problem	66
Klyucharev P. G. Deterministic methods of Ramanujan graph construction for use in cryptographic algorithms based on generalized cellular automata	76
COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS	
Kuznetsov A. A., Kuznetsova A. S. A resource-efficient algorithm for study the growth in finite two-generator groups of exponent 5	94
DISCRETE MODELS FOR REAL PROCESSES	
Hazdiuk Ye. P., Zhikharevich V. V., Nikitina O. M., Ostapov S. E. The unicellular microorganisms "Amoeba Proteus" locomotion simulation with the use of movable cellular automata method	104
MATHEMATICAL BACKGROUNDS OF INTELLIGENT SYSTEMS	
Nefedov V. N., Smerchinskaya S. O., Yashina N. P. Constructing an aggre- gated relation with a minimum distance from the expert preferences	120
BRIEF INFORMATION ABOUT THE AUTHORS	133