

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2017

№ 38

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, 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); 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 12.12.2017. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 15,48. Тираж 300 экз.
Заказ № 2909. Цена свободная. Дата выхода в свет 26.12.2017.

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

Чередник И. В. Один подход к построению транзитивного множества блочных преобразований	5
Шулежко О. В., Панов Н. П. О почти нильпотентных многообразиях антикоммутативных метабелевых алгебр	35
Shevlyakov A. N. On irreducible algebraic sets over linearly ordered semilattices II	49

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Agibalov G. P. Substitution block ciphers with functional keys	57
---	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Попков К. А. Единичные проверяющие тесты для схем из функциональных элементов в базисе «конъюнкция-отрицание»	66
--	----

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Абросимов М. Б., Моденова О. В. О минимальных вершинных 1-расширениях ориентаций цепей	89
---	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Рыбалов А. Н. О генерической сложности проблемы извлечения корня в группах вычетов	95
Сафонов В. О., Стефанцов Д. А. Комплексы в ЛЯПАСе	101

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Адельшин А. В., Кучин А. К. Исследование L -структуры многогранника смешанной задачи максимальной выполнимости	110
Кочергин В. В., Кочергин Д. В. Уточнение нижней оценки сложности возведения в степень	119
СВЕДЕНИЯ ОБ АВТОРАХ	133

CONTENTS

THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

Cherednik I. V. One approach to constructing a transitive class of block transformations	5
Shulezhko O. V., Panov N. P. On almost nilpotent varieties of anticommutative metabelian algebras	35
Shevlyakov A. N. On irreducible algebraic sets over linearly ordered semilattices II	49

MATHEMATICAL METHODS OF CRYPTOGRAPHY

Agibalov G. P. Substitution block ciphers with functional keys	57
---	----

MATHEMATICAL BACKGROUNDS OF COMPUTER AND CONTROL SYSTEM RELIABILITY

Popkov K. A. Single fault detection tests for logic networks of AND, NOT gates	66
---	----

APPLIED GRAPH THEORY

Abrosimov M. B., Modenova O. V. On minimal vertex 1-extensions of path orientation	89
---	----

MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

Rybalov A. N. On generic complexity of the problem of finding roots in groups of residues	95
Safonov V. O., Stefantsov D. A. Complexes in LYaPAS	101

COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

Adelshin A. V., Kuchin A. K. Analysis of L -structure of polyhedron in the partial MAX SAT problem	110
Kochergin V. V., Kochergin D. V. Improvement of the lower bound for the complexity of exponentiation	119
BRIEF INFORMATION ABOUT THE AUTHORS	133