

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2014

№1(23)

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, проф. (зам. председателя); Парватов Н. Г., д-р физ.-мат. 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.; Закревский А. Д., д-р техн. наук, проф., чл.-корр. НАН Беларуси; Колесникова С. И., д-р техн. наук; Костюк Ю. Л., д-р техн. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; 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 надежности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*

Верстка *И. А. Панкратовой*

Подписано к печати 11.03.2014.

Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз.

Издательство ТГУ. 634029, Томск, ул. Никитина, 4

СОДЕРЖАНИЕ

ПАМЯТИ УЧИТЕЛЯ	5
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ	
Аборнев А. В. Построение подстановок с использованием разрядно-подстановочных преобразований модуля над кольцом Галуа характеристики 4	9
Фомичев В. М. Эквивалентные по Фробениусу примитивные множества чисел	20
МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ	
Рожков М. И. Биективные отображения, порождаемые фильтрующим генератором	27
Шушуев Г. И. Поиск оптимального линейного приближения сетей Фейстеля	40
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	
Сорокин С. Н. Метод обнаружения атак типа «отказ в обслуживании» на web-приложения	55
ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ	
Покровский А. В. О весовых спектрах одного класса линейных кодов	65
Таранников Ю. В. О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$	73
ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ	
Дорохова А. М., Фомичев В. М. Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов	77
Корниенко А. С. Структура функциональных графов для циркулянтов с линейными булевыми функциями в вершинах	84
ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ	
Дюкова Е. В., Прокофьев П. А. Об асимптотически оптимальном перечислении неприводимых покрытий булевой матрицы	96
Pottosin Yu. V., Kardash S. N. Pipelining combinational circuits	106
ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ	
Афанасьев И. В. Применение КА-модели для исследования влияния загрязнений на динамику популяций голомянок и макрогектопуса в озере Байкал	114
СВЕДЕНИЯ ОБ АВТОРАХ	124
АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ	125