

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2012

№3(17)

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., канд. 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.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Евтушенко Н. В., д-р техн. наук, проф.; Закревский А. Д., д-р техн. наук, проф., чл.-корр. НАН Беларуси; Костюк Ю. Л., д-р техн. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Матросова А. Ю., д-р техн. 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.; 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 10.09.2012.

Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13. Уч.-изд. л. 14,5. Тираж 300 экз.

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

Отпечатано в типографии ТПУ.

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Едемский В. А., Антонова О. В. Линейная сложность обобщённых циклотомических последовательностей с периодом $2^m p^n$	5
Ерофеев С. Ю., Романьков В. А. О построении возможно односторонних функций на основе алгоритмической неразрешимости проблемы эндоморфной сводимости в группах	13
Солодовников В. И. О совпадении класса бент-функций с классом функций, минимально близких к линейным	25

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Коренева А. М., Фомичев В. М. Об одном обобщении блочных шифров Фейстеля ...	34
Рацеев С. М. О совершенных имитостойких шифрах	41
Тужилин М. Э. Латинские квадраты и их применение в криптографии	47
Черемушкин А. В. О содержании понятия «электронная подпись»	53

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Колегов Д. Н. Построение иерархического ролевого управления доступом	70
--	----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Агибалов Г. П. К возрождению русского языка программирования	77
--	----

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Монахов О. Г. Исследование влияния степени специализации шаблона на пространство поиска при эволюционном синтезе моделей	85
Мурин Д. М. О некоторых свойствах образов трансформированных задач	96

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Цициашвили Г. Ш., Лосев А. С. Связность планарного графа с высоконадёжными рёбрами	103
--	-----

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Бандман О. Л. Инварианты клеточно-автоматных моделей реакционно-диффузионных процессов	108
--	-----

СВЕДЕНИЯ ОБ АВТОРАХ	121
---------------------------	-----

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ	123
--	-----