

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2011

№3(13)

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 (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.; 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.; Микони С. В., 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 26.08.2011.

Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,8. Уч.-изд. л. 15,47. Тираж 300 экз.

Отпечатано в типографии ТПУ.

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Алексейчук А. Н., Шевцов А. С. Быстрый алгоритм статистического оценивания максимальной несбалансированности билинейных аппроксимаций булевых отображений.....	5
Вороненко А. А. О сложности доказательства повторности булевых функций в бинарном базисе.....	12
Гречников Е. А. Метод комплексного умножения для построения эллиптических кривых и его оптимизации	17

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Стефанцов Д. А. Внедрение политик безопасности в программные системы обработки информации	55
--	----

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Быкова В. В. Вычислительные аспекты древовидной ширины графа	65
Ильев В. П., Навроцкая А. А. Вычислительная сложность задачи аппроксимации графами с компонентами связности ограниченного размера	80
Магомедов А. М., Магомедов Т. А. Интервальная на одной доле правильная реберная 5-раскраска двудольного графа.....	85
Монахова Э. А. Структурные и коммуникативные свойства циркулянтных сетей	92

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Фомичев В. М. О реализации метода согласования в криптоанализе с помощью параллельных вычислений	116
---	-----

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

Киселев И. С. Аналитический метод доопределения кратных предпочтений в матрице парных сравнений	122
--	-----

СВЕДЕНИЯ ОБ АВТОРАХ	129
---------------------------	-----

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ	130
--	-----