

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2010

№3(9)

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.

ООО «Издательство научно-технической литературы»

634050, Томск, пл. Ново-Соборная, 1, тел. (3822) 533-335

Редактор *Н. И. Шидловская*

Верстка *Д. А. Стефанцова*

Изд. лиц. ИД. №04000 от 12.02.2001. Подписано к печати 15.09.2010.
Формат 60 × 84 $\frac{1}{8}$. Бумага офсетная. Печать офсетная. Гарнитура «Таймс».
Усл. п. л. 13,2. Уч.-изд. л. 14,8. Тираж 300 экз. Заказ №17.

Отпечатано в типографии «М-Принт», г. Томск, ул. Пролетарская, 38/1

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Егоров В. Н. О группах автоморфизмов матриц	5
Логачев О. А. О значениях уровня аффинности для почти всех булевых функций	17
Парватов Н. Г. Точечные и сильно точечные функции на полурешётке	22
Смышляев С. В. Построение классов совершенно уравновешенных булевых функций без барьера	41

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Агибалов Г. П., Панкратова И. А. Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров	51
Тренькаев В. Н. Реализация шифра Закревского на основе перестраиваемого автомата	69

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Качанов М. А. Анализ безопасности информационных потоков в операционных системах семейства <i>GNU/Linux</i>	77
Паутов П. А. Аутентификация в модели доверенной подсистемы на основе ком- мутативного шифрования	90

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Долгов А. А. Семейство точных 2-расширений турниров	96
---	----

ЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ ДИСКРЕТНЫХ АВТОМАТОВ

Чеботарёв А. Н. Решение неравенств над автоматами в проектировании реак- тивных систем	100
---	-----

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

Бандман О. Л., Громилов С. А., Кинеловский С. А. Кумулятивный синтез: клеточно-автоматная модель процесса образования покрытия, наносимого на мишень с помощью кумулятивного потока частиц	111
СВЕДЕНИЯ ОБ АВТОРАХ	121
АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ	123