

# **ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА**

---

---

*Научный журнал*

---

---

**2008**

**№1(1)**



ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

## НАУЧНО-РЕДАКЦИОННЫЙ СОВЕТ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Майер Г.В., д-р физ.-мат. наук, проф. (председатель); Дунаевский Г.Е., д-р техн. наук, проф. (зам. председателя); Ревушкин А.С., д-р биол. наук, проф. (зам. председателя); Катунин Д.А., канд. филол. наук, доц. (отв. секретарь); Аванесов С.С., д-р филос. наук, проф.; Берцун В.Н., канд. физ.-мат. наук, доц.; Гага В.А., д-р экон. наук, проф.; Галажинский Э.В., д-р психол. наук, проф.; Глазунов А.А., д-р техн. наук, проф.; Голиков В.И., канд. ист. наук, доц.; Горцев А.М., д-р техн. наук, проф.; Гураль С.К., канд. филол. наук, проф.; Демешкина Т.А., д-р филол. наук, проф.; Демин В.В., канд. физ.-мат. наук, доц.; Ершов Ю.М., канд. филол. наук, доц.; Зиновьев В.П., д-р ист. наук, проф.; Канов В.И., д-р экон. наук, проф.; Кривова Н.А., д-р биол. наук, проф.; Кузнецов В.М., канд. физ.-мат. наук, доц.; Кулижский С.П., д-р биол. наук, проф.; Парначев В.П., д-р геол.-минерал. наук, проф.; Петров Ю.В., д-р филос. наук, проф.; Портнова Т.С., канд. физ.-мат. наук, директор Издательства НТЛ; Потеев А.И., д-р физ.-мат. наук, проф.; Прокументов Л.М., д-р юрид. наук, проф.; Прокументова Г.Н., д-р пед. наук, проф.; Савицкий В.К., зав. редакционно-издательским отделом; Сахарова З.Е., канд. экон. наук, доц.; Слизов Ю.Г., канд. хим. наук, доц.; Сумарокова В.С., директор Издательства ТГУ; Сущенко С.П., д-р техн. наук, проф.; Тарасенко Ф.П., д-р техн. наук, проф.; Татьяна Г.М., канд. геол.-минерал. наук, доц.; Унгер Ф.Г., д-р хим. наук, проф.; Уткин В.А., д-р юрид. наук, проф.; Шилько В.Г., д-р пед. наук, проф.; Шрагер Э.Р., д-р техн. наук, проф.

### РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА «ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»

Агibalов 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, проф. (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; 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.; 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 ее приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании и теории надежности.*

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.В. Фортес*

К-ОКП ОК-005-93, код продукции 952000

---

Изд. лиц. ИД № 04000 от 12.02.2001. Подписано к печати 18.06.2008.  
Формат 70 × 100 <sup>1</sup>/<sub>16</sub>. Бумага офсетная. Печать офсетная. Гарнитура «Таймс».  
Усл. п. л. 9,35. Уч.-изд. л. 10,48. Тираж 300 экз. Заказ № 7.

---

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

## СОДЕРЖАНИЕ<sup>1</sup>

О ЖУРНАЛЕ.....	5
----------------	---

### ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Горшков С.П. О сложности нахождения приведенных представлений слабо положительных и слабо отрицательных булевых функций .....	7
Иванов А.В. Мономиальные приближения платовидных функций.....	10
Куткин А.М. Коды, композиции и решетки.....	15
Кыров В.А. Трехбазисные квазигруппы с обобщенным тождеством Уорда .....	21
Пудовкина М.А. Линейные структуры групп подстановок над конечным модулем.....	25
Шоломов Л.А. Энтропия недоопределенных последовательностей при ограничениях на доопределения.....	29

### МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Агibalов Г.П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом .....	34
Росошек С.К., Боровков А.А., Евсютин О.О. Криптосистемы клеточных автоматов.....	43
Токарева Н.Н. Квадратичные аппроксимации специального вида для четырехразрядных подстановок в S-блоках.....	50
Черемушкин А.В. Комбинаторно-геометрические подходы к построению схем предварительного распределения ключей (обзор).....	55

### МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Девянин П.Н. Базовая ролевая ДП-модель .....	64
Колегов Д.Н. Применение ДП-моделей для анализа защищенности сетей .....	71
Кучеров М.М., Кирко И.Н., Муллер А.А. Современные модели и механизмы защиты информации .....	88
Стефанцов Д.А. Реализация политик безопасности в компьютерных системах с помощью аспектно-ориентированного программирования .....	94

### ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

Абросимов М.Б., Долгов А.А. Семейства точных расширений турниров .....	101
Евдокимов А.А., Левин А.А. Инструментарий графического исследования символьных последовательностей .....	108
Наumenko И.А., Скобелев В.Г. Преобразование решёток в 1-отказоустойчивые графы.....	111
Салий В.Н. Минимальные примитивные расширения ориентированных графов.....	116

### ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

Бушков В.Г. К описанию прогрессивных решений параллельного автоматного уравнения .....	120
Скобелев В.В. Характеристика неподвижных точек линейных автоматов над конечным кольцом.....	126
Сухинин В.А., Скобелев В.Г. Идентификация автомата в классе автоматов Спротта.....	131

СВЕДЕНИЯ ОБ АВТОРАХ.....	136
--------------------------	-----

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ .....	138
--	-----

<sup>1</sup> Статьи этого номера представлены оргкомитетом VII Сибирской научной школы-семинара с международным участием «Компьютерная безопасность и криптография» – SIBECRYPT'08. Школа-семинар проведена совместно Томским госуниверситетом и Сибирским государственным аэрокосмическим университетом в сотрудничестве с Институтом криптографии, связи и информатики Академии ФСБ с 9 по 12 сентября 2008 года в г. Красноярске при финансовой поддержке РФФИ (грант № 08-07-06024-г).