

# **ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА**

---

---

*Научный журнал*

---

---

**2008**

**№ 2(2)**



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 физ.-мат. 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; Потехаев А.И., д-р физ.-мат. наук, проф.; Прозументов Л.М., д-р юрид. наук, проф.; Прозументова 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*

---

Изд. лиц. ИД № 04000 от 12.02.2001. Подписано к печати 12.08.2008.  
Формат 70 × 100 <sup>1</sup>/<sub>16</sub>. Бумага офсетная. Печать офсетная. Гарнитура «Таймс».  
Усл. п. л. 16,04. Уч.-изд. л. 17,97. Тираж 300 экз. Заказ № 7.

---

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

# СОДЕРЖАНИЕ<sup>1</sup>

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

<b>Былков Д.Н.</b> Расстояние единственности семейства координатных последовательностей, полученных усложнением линейных рекуррент над кольцом Галуа .....	5
<b>Егорушкин О.И., Калугин-Балашов Д.А., Сафонов К.В.</b> О решении систем алгебраических уравнений, ассоциированных с контекстно-свободными языками .....	8
<b>Мурадов Р.М., Кыров В.А.</b> О квазигруппах, возникающих из физической структуры ранга (2, 2) .....	12
<b>Поздеев А.Г.</b> Построение нормальных периодических последовательностей из циклически минимальных чисел .....	15
<b>Тужилин М.Э.</b> Алгебраический иммунитет булевых функций .....	18
<b>Фомичев В.М.</b> О $\sigma$ -ширине конечных ациклических групп .....	23

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

<b>Глухов М.М.</b> О применениях квазигрупп в криптографии .....	28
<b>Ивашенко Е.А., Скобелев В.Г.</b> Представление криптосистем многоосновной алгебраической системой .....	33
<b>Ковалев А.М., Козловский В.А., Щербак В.Ф.</b> Обратимые динамические системы с переменной размерностью фазового пространства в задачах криптографического преобразования информации .....	39
<b>Кукарцев А.М., Попов А.М., Шестаков В.С.</b> О прямом операционном анализе симметричных шифров .....	45
<b>Парватов Н.Г.</b> Совершенные схемы разделения секрета .....	50
<b>Пудовкина М.А.</b> Свойства некоторых алгоритмов шифрования Фейстеля относительно двух групп сплетения .....	58
<b>Скобелев В.Г.</b> Анализ атак на квантовый протокол передачи ключа .....	62

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

<b>Гришин А.М.</b> Методы защиты речевой информации .....	67
<b>Золотарев В.В., Ширкова Е.А.</b> Фундаментальные основы методик базового экспертного анализа информационных рисков .....	71
<b>Качанов М.А., Колегов Д.Н.</b> Расширение функциональности системы безопасности ядра Linux на основе подмены системных вызовов .....	76
<b>Колегов Д.Н., Чернушенко Ю.Н.</b> О соревнованиях CTF по компьютерной безопасности .....	81
<b>Лапшин В.В.</b> О централизованном территориально-распределённом анализе сетевого трафика .....	84
<b>Паутов П.А.</b> Проблема аутентификации в многоуровневых приложениях .....	87
<b>Пестунова Т.М., Родионова З.В.</b> Управление процессом предоставления прав доступа на основе анализа бизнес-процессов .....	91

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЕЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

<b>Димитриев Ю.К.</b> Эффективность локального самодиагностирования в вычислительных системах с циркулянтной диагностической структурой .....	96
<b>Мелентьев В.А.</b> Функция структурной отказоустойчивости и $d$ -ограниченная компонента связности графа вычислительной системы .....	102
<b>Мелентьев В.А.</b> Поиск вершинных $(s, t)$ -сечений графа вычислительной системы с ограничением по диаметру компонент связности .....	107

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

<b>Дулькейт В.И., Файзуллин Р.Т., Хныкин И.Г.</b> Минимизация функционалов, ассоциированных с задачами криптографического анализа асимметричных шифров .....	113
<b>Семенов А.А., Заикин О.С., Беспалов Д.В., Буров П.С., Хмельнов А.Е.</b> Анализ некоторых криптографических примитивов на вычислительных кластерах .....	120

## ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

<b>Потапов В.Н.</b> Арифметическое кодирование сообщений с использованием случайных последовательностей .....	131
<b>СВЕДЕНИЯ ОБ АВТОРАХ</b> .....	134
<b>АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ</b> .....	136

<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).