

# ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

---

---

*Приложение*

---

---

№ 9

Сентябрь 2016

Свидетельство о регистрации: ПИ № ФС 77-50702  
от 17 июля 2012 г.

ТРУДЫ  
Всероссийской конференции  
«XV Сибирская научная школа-семинар с международным участием  
“Компьютерная безопасность и криптография” — SIBECRYPT’16»  
(Новосибирск, 5–10 сентября 2016 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); 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.; Быкова В. В., д-р физ.-мат. наук, проф.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Колесникова С. И., д-р техн. наук; Крылов П. А., д-р физ.-мат. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Мясников А. Г., д-р физ.-мат. наук, проф.; Романьков В. А., д-р физ.-мат. 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.; Шойтов А. М., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ; Шоломов Л. А., д-р физ.-мат. наук, проф.

Адрес редакции: 634050, г. Томск, пр. Ленина, 36  
E-mail: vestnik\_pdm@mail.tsu.ru

*Всероссийская конференция «XV Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография” — SIBECRYPT’16» проведена Национальным исследовательским Томским государственным университетом и Институтом математики СО РАН им. С. Л. Соболева в сотрудничестве с Институтом криптографии, связи и информатики с 5 по 10 сентября 2016 г. в Новосибирске при финансовой поддержке РФФИ (грант № 16-07-20516-г).*

Теоретические основы прикладной дискретной математики  
Дискретные функции  
Математические методы криптографии  
Математические основы компьютерной безопасности  
Математические основы надёжности вычислительных  
и управляющих систем  
Прикладная теория автоматов и графов  
Математические основы информатики и программирования  
Вычислительные методы в дискретной математике

Редактор *Н. И. Шидловская*  
Верстка *И. А. Панкратовой*

---

Подписано к печати 09.08.2016.  
Формат 60 × 84 $\frac{1}{8}$ . Усл. п. л. 15,9. Уч.-изд. л. 17,8. Тираж 300 экз. Заказ № 2000.

---

Отпечатано на оборудовании  
Издательского Дома Томского государственного университета  
634050, г. Томск, пр. Ленина, 36  
Тел.: 8(3822)53-15-28, 52-98-49

# СОДЕРЖАНИЕ

## Секция 1

### ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

<b>Бондаренко Л. Н., Шарапова М. Л.</b> Обобщённые многочлены Нараяны и их $q$ -аналоги.....	6
<b>Волгин А. В.</b> Об одном критерии проверки гипотезы о наличии вкраплений в двоичной цепи Маркова .....	9
<b>Евдокимов А. А.</b> Алгоритм распознавания полноты множества слов и динамика запретов .....	10
<b>Кузьмин С. А.</b> О достаточном условии для отсутствия возможности сокращения периода в старших двоичных разрядных последовательностях над примарными кольцами.....	12
<b>Погорелов Б. А., Пудовкина М. А.</b> О группах, порождённых преобразованиями смешанного типа и группами наложения ключа .....	14
<b>Погорелов Б. А., Пудовкина М. А.</b> О классификации дистанционно-транзитивных графов орбиталов надгруппы группы Джевонса.....	16

## Секция 2

### ДИСКРЕТНЫЕ ФУНКЦИИ

<b>Виткуп В. А.</b> О специальном подклассе векторных булевых функций и проблеме существования APN-перестановок.....	19
<b>Городилова А. А.</b> О дифференциальной эквивалентности квадратичных APN-функций.....	21
<b>Зуева И. А., Карпов В. А.</b> Функции с вариационно-координатной полиномиальностью над группой .....	24
<b>Коломеец Н. А.</b> О расстоянии Хэмминга между двумя бент-функциями .....	27
<b>Куценко В. А.</b> О множестве расстояний Хэмминга между самодуальными бент-функциями .....	29
<b>Покрасенко Д. П.</b> Условия существования векторной булевой функции с максимальной компонентной алгебраической иммунностью .....	30
<b>Сошин Д. А.</b> Представление полубайтовых подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ алгебраическими пороговыми функциями.....	32
<b>Токарева Н. Н.</b> О множестве производных булевой бент-функции .....	35
<b>Черемушкин А. В.</b> О распределении ранга и оценке уровня аффинности квадратичных форм.....	36
<b>Шушуев Г. И.</b> Функции на расстоянии один от APN-функций от малого числа переменных .....	39

## Секция 3

### МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

<b>Агибалов Г. П., Панкратова И. А.</b> К криптоанализу двухкаскадных конечно-автоматных криптографических генераторов .....	41
<b>Власова В. В., Пудовкина М. А.</b> О группе, порождённой раундовыми функциями алгоритма блочного шифрования «Кузнечик» .....	43

<b>Заикин О. С., Отпущенников И. В., Семёнов А. А.</b> Оценки стойкости шифров семейства Trivium к криптоанализу на основе алгоритмов решения проблемы булевой выполнимости .....	46
<b>Коренева А. М., Мартышин В. Н.</b> Экспериментальное исследование экспонентов раундовых перемешивающих матриц обобщённых сетей Фейстеля.....	48
<b>Коренева А. М., Фомичёв В. М.</b> О существенных переменных функции переходов модифицированного аддитивного генератора .....	51
<b>Косолапов Ю. В., Турченко О. Ю.</b> Поиск информационного сообщения в зашумлённых кодовых блоках при многократной передаче данных.....	55
<b>Кяжин С. Н., Лебедев Ф. В.</b> О точности матрично-графового подхода к оценке перемешивающих свойств преобразований .....	57
<b>Кяжин С. Н., Фомичев В. М.</b> Перемешивающие свойства двухкаскадных генераторов.....	60
<b>Медведева Н. В., Титов С. С.</b> Аналоги теоремы Шеннона для эндоморфных неминимальных шифров .....	62
<b>Романько Д. А., Фомичев В. М.</b> О способах построения криптографических генераторов с заданным показателем неповторности выходных последовательностей.....	65
<b>Рябко Б. Я.</b> Применение двуликих процессов к генерированию псевдослучайных чисел.....	68
<b>Фомичев М. В.</b> О ключевом расписании блочных шифров без слабых ключей .....	70
<b>Чижов И. В., Бородин М. А.</b> Криптоанализ криптосистемы Мак-Элиса, построенной на $(k - 1)$ -подкодах кода Риды — Маллера .....	73

## Секция 4

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ**

<b>Анисеня Н. И.</b> Протокол безотказной луковой маршрутизации с подтверждением времени создания сообщения .....	76
<b>Горбатенко Д. Е., Кочемазов С. Е., Семёнов А. А.</b> О дискретно-автоматных моделях атак в компьютерных сетях .....	80
<b>Девянин П. Н.</b> О результатах формирования иерархического представления МРОСЛ ДП-модели .....	83
<b>Кащеев М. Р., Косолапов Ю. В.</b> Схема обеспечения конфиденциальности в алгоритме RAID-PIR.....	87
<b>Колегов Д. Н., Брославский О. В., Олексов Н. Е.</b> Метод запутывания программной реализации схемы НМАС для недоверенной среды .....	89
<b>Колегов Д. Н., Линейцев П. А.</b> Об идентификации защитных экранов веб-приложений в модели MitB .....	92
<b>Колегов Д. Н., Ткаченко Н. О.</b> Легковесная реализация механизма атрибутного управления доступом для СУБД на уровне защитного экрана .....	93

## Секция 5

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ**

<b>Алехина М. А., Барсукова О. Ю.</b> О надёжности схем в базисе Россера — Туркетта (в $P_k$ ).....	96
<b>Алехина М. А., Логвина О. А.</b> Ненадёжность схем при слипаниях входов элементов. 98	

## Секция 6

**ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ**

<b>Абросимов М. Б., Моденова О. В.</b> Уточнение нижней оценки числа дополнительных дуг минимального вершинного 1-расширения ориентации цепи.....	101
<b>Абросимов М. Б., Сухов С. А.</b> О количестве оптимальных 1-гамильтоновых графов с числом вершин до 26 и 28.....	103
<b>Авезова Э. Я., Фомичев М. В.</b> Об одном наследственном признаке в циклических полугруппах графов .....	105
<b>Воблый В. А., Мелешко А. К.</b> Перечисление помеченных цветочно-колёсных графов .....	109
<b>Евдокимов А. А., Куценогая Е. П., Федоряева Т. И.</b> О графах полного раз- нообразия шаров .....	110
<b>Жаркова А. В.</b> Об аттракторах в конечных динамических системах ориентаций полных графов.....	112
<b>Жуковская А. О., Тренькаев В. Н.</b> О простых условных экспериментах иден- тификации обратимых автоматов некоторого класса .....	115
<b>Карандашов М. В.</b> О транзитивности отображений, ассоциированных с конеч- ными автоматами из групп $AS_p$ .....	115

## Секция 7

**МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ  
И ПРОГРАММИРОВАНИЯ**

<b>Егорушкин О. И., Колбасина И. В., Сафонов К. В.</b> О совместности систем символьных полиномиальных уравнений и их приложения .....	119
<b>Князев В. Н., Князева М. С.</b> Транслятор языка ЛЯПАС-Т на язык ассемблера для ОС Windows и Linux .....	121
<b>Стефанцов Д. А., Сафонов В. О., Першин В. В., Гречнев С. Ю., Том- ских П. А.</b> Модульный транслятор с языка ЛЯПАС .....	122
<b>Чушкин М. С., Шелехов В. И.</b> Методы синтеза фрагментов предикатных программ.....	126

## Секция 8

**ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ**

<b>Грибанова И. А.</b> Применение алгоритмов решения проблемы булевой выполни- мости к построению разностных путей в задачах поиска коллизий криптогра- фических хеш-функций семейства MD .....	129
<b>Кузнецов А. А., Карчевский С. С.</b> О вычислении функций роста конечных двупорождённых бернсайдовых групп периода 5 .....	132
<b>СВЕДЕНИЯ ОБ АВТОРАХ .....</b>	136
<b>АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ .....</b>	141