

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»**

Агibalов 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 $60 \times 84\frac{1}{8}$. 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

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

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

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

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

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

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

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

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

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

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

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ

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

Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ
И ПРОГРАММИРОВАНИЯ

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

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

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