

# **ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА**

---

---

*Научный журнал*

---

---

2017

№ 37

Зарегистрирован в Федеральной службе по надзору  
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

**УЧРЕДИТЕЛЬ**  
**Томский государственный университет**

**РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА**  
**«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»**

Агибалов Г. П., д-р техн. наук, проф. (главный редактор); Девянин П. Н., д-р техн. наук, чл.-корр. Академии криптографии РФ (зам. гл. редактора); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. гл. редактора); 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, доц.; Фомичев В. М., д-р физ.-мат. наук, проф.; Харин Ю. С., д-р физ.-мат. наук, чл.-корр. НАН Беларуси; Чеботарев А. Н., д-р техн. наук, проф.; Шоломов Л. А., д-р физ.-мат. наук, проф.

**Адрес редакции и издателя:** 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 надёжности, интеллектуальных системах.*

Периодичность выхода журнала: 4 номера в год.

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

---

Подписано к печати 20.09.2017. Формат  $60 \times 84\frac{1}{8}$ . Усл. п. л. 14,55. Тираж 300 экз.  
Заказ № 2743. Цена свободная. Дата выхода в свет 04.10.2017.

---

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

# СОДЕРЖАНИЕ

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

<b>Анохин М. И.</b> О двух определениях степени функции над ассоциативным коммутативным кольцом .....	5
<b>Novoselov S. A.</b> Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials .....	20

## МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

<b>Коренева А. М.</b> О примитивности перемешивающих орграфов биективных регистров сдвига с двумя обратными связями .....	32
<b>Романьков В. А., Обзор А. А.</b> Общая алгебраическая схема распределения криптографических ключей и её криптоанализ .....	52

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

<b>Алехина М. А., Барсукова О. Ю.</b> Оценки ненадёжности схем в базисе Россе-ра — Туркетта (в $P_3$ ) при неисправностях типа 0 на выходах элементов .....	62
---	----

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

<b>Егорушкин О. И., Колбасина И. В., Сафонов К. В.</b> О применении многомерного комплексного анализа в теории формальных языков и грамматик .....	76
<b>Костюк Ю. Л.</b> Эффективная трансляция для LL(1)-грамматики на примере языка программирования .....	90
<b>Рыбалов А. Н.</b> О генерической сложности проблемы разрешимости систем дифантовых уравнений в форме Сколема .....	100
<b>Тарков М. С.</b> Редукция связей автоассоциативной памяти Хопфилда .....	107

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

<b>Быкова В. В., Солдатенко А. А.</b> Оптимальная маршрутизация по ориентирам в нестационарных сетях .....	114
<b>СВЕДЕНИЯ ОБ АВТОРАХ</b> .....	124

# CONTENTS

## THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS

<b>Anokhin M. I.</b> On the two definitions of degree of a function over an associative, commutative ring .....	5
<b>Novoselov S. A.</b> Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials .....	20

## MATHEMATICAL METHODS OF CRYPTOGRAPHY

<b>Koreneva A. M.</b> On primitivity of mixing digraphs associated with 2-feedbacks shift registers .....	32
<b>Roman'kov V. A., Obzor A. A.</b> General algebraic cryptographic key exchange scheme and its cryptanalysis .....	52

## MATHEMATICAL BACKGROUNDS OF COMPUTER AND CONTROL SYSTEM RELIABILITY

<b>Alekhina M. A., Barsukova O. Yu.</b> Estimations of unreliability of circuits in Rosser — Turkett basis (in $P_3$ ) with faults of type 0 at the outputs of gates .....	62
--	----

## MATHEMATICAL BACKGROUNDS OF INFORMATICS AND PROGRAMMING

<b>Egorushkin O. I., Kolbasina I. V., Safonov K. V.</b> On application of multidimensional complex analysis in formal language and grammar theory .....	76
<b>Kostyuk Yu. L.</b> Effective translation for LL(1)-grammar in the example of a programming language .....	90
<b>Rybalov A. N.</b> On generic complexity of decidability problem for diophantine systems in the Skolem's form .....	100
<b>Tarkov M. S.</b> Reduction of synapses in the Hopfield autoassociative memory .....	107

## COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS

<b>Bykova V. V., Soldatenko A. A.</b> Optimal routing by landmarks in the time-dependent networks .....	114
BRIEF INFORMATION ABOUT THE AUTHORS .....	124