

Российская академия наук

ПРОГРАММИРОВАНИЕ

№ 4 2024 Июль—Август

Основан в 1975 г.
Выходит 6 раз в год
ISSN: 0132-3474

Индекс журнала «Программирование»
в каталоге Респечати 39391

*Журнал издается под руководством
Отделения математических наук РАН*

Главный редактор
А. И. Аветисян

Заместитель главного редактора
А. К. Петренко

Редакционная коллегия:

С. А. Абрамов, И. Б. Вирбицкайте,
К. В. Воронцов, В. А. Галактионов, Ф. Я. Дзержинский,
Л. Е. Карпов (ответственный секретарь),
М. Р. Когаловский, А. С. Косачев, И. В. Машечкин,
Б. А. Новиков, А. Н. Прокопья, В. А. Серебряков

Подписка на журнал принимается без ограничения
всеми отделениями «Респечати» (№ 39391 в каталоге).

Заведующая редакцией **Т.А. Оловянникова**

119991 Москва, Ленинские горы, д. 1, стр. 52
МГУ, факультет вычислительной математики и кибернетики
109004 Москва, ул. А. Солженицына, д. 25
Институт системного программирования им. В.П. Иванникова РАН
E-mail: progr@ispras.ru

СОДЕРЖАНИЕ

Номер 4, 2024

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сравнительный анализ эффективности алгоритмов хэширования
с точки зрения применения в системах zk-SNARK в распределенных реестрах

Д. О. Кондырев 3

КОМПЬЮТЕРНАЯ ГРАФИКА И ВИЗУАЛИЗАЦИЯ

Построение внутренней диаграммы Вороного многоугольной фигуры
методом заметания

Л. М. Местецкий, Д. А. Коптелов 13

ПРОГРАММНАЯ ИНЖЕНЕРИЯ, ТЕСТИРОВАНИЕ И ВЕРИФИКАЦИЯ ПРОГРАММ

Аналитический обзор конфиденциального искусственного интеллекта:
методы и алгоритмы реализации в облачных вычислениях

Е. М. Ширяев, А. С. Назаров, Н. Н. Кучеров, М. Г. Бабенко 27

RuGESToR: нейросетевая модель на основе правил
для исправления грамматических ошибок на русском языке

*И. А. Хабутдинов, А. В. Чащин, А. В. Грабовой,
А. С. Кильдяков, Ю. В. Чехович* 41

Contents

No. 4, 2024

INFORMATION SECURITY

Comparative Efficiency Analysis of Hashing Algorithms for Applications
in zk-SNARK Circuits in Distributed Ledgers

D. O. Kondyrev

3

COMPUTER GRAPHICS AND VISUALIZATION

Constructing the Internal Voronoi Diagram of a Polygonal Figure
Using the Sweep Method

L. M. Mestetskiy, D. A. Koptelov

13

SOFTWARE ENGINEERING, TESTING AND VERIFICATION

Analytical Review of Confidential Artificial Intelligence:
Methods and Algorithms for Deployment in Cloud Computing

E.M. Shiriaev, A.S. Nazarov, N.N. Kuchеров, M.G. Babenko

27

RuGECToR: Rule-Based Neural Network Model for Russian Language
Grammatical Error Correction

*I. A. Khabutdinov, A. V. Chashchin, A. V. Grabovoy,
A. S. Kildyakov, Y. V. Chekhovich*

41
