

Российская академия наук

ПРОГРАММИРОВАНИЕ

№ 6 2024 Ноябрь—Декабрь

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. Оловяникова**

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 6, 2024

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Высокоскоростной алгоритм скалярного умножения для проектирования нейронных сетей, сохраняющих конфиденциальность	
<i>М. А. Лапина, Е. М. Ширяев, М. Г. Бабенко, И. Истамов</i>	3
Алгоритмы размещения и запроса к конфиденциальным данным на облаке	
<i>Н. П. Варновский, С. А. Мартишин, М. В. Храпченко, А. В. Шокуров</i>	12

АНАЛИЗ ДАННЫХ

Адаптивный БИХ-фильтр на базе штрафного сплайна	
<i>Е. А. Кочегурова, Ю. А. Мартынова</i>	24
Дискретный алгоритм оптимизации на основе распределения вероятностей с трансформацией целевых значений	
<i>К. С. Сарин</i>	35
Оптимизация быстродействия программного обеспечения реализации алгоритмов классификации и привязки деловых документов	
<i>О. А. Славин</i>	48

Contents

No. 6, 2024

INFORMATION SECURITY

High-Speed Convolution Core Architecture for Privacy-Preserving Neural Networks <i>M. A. Lapina, E. M. Shiriaev, M. G. Babenko, I. Istamov</i>	3
Cloud Data Placing and Private Information Retrieval Algorithms <i>N. P. Varnovskiy, S. A. Martishin, M. V. Khrapchenko, A. V. Shokurov</i>	12

DATA ANALYSIS

Adaptive IIR Filter Based on Penalized Spline <i>E. A. Kochegurova, I. A. Martynova</i>	24
Discrete Optimization Algorithm Based on Probability Distribution with Transformation of Target Values <i>K. S. Sarin</i>	35
Optimization of Software Performance for Classification and Linking of Administrative Documents <i>O. A. Slavin</i>	48