

Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам'янець-Подільський національний університет
імені Івана Огієнка

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Серія: Технічні науки

Збірник наукових праць

Випуск 19

Кам'янець-Подільський національний університет
імені Івана Огієнка
2019

УДК 004.94:53.072
ББК 30
М34

Свідцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 14522-3493Р від 25.06.2008 р.

Збірник наукових праць включено до Переліку наукових фахових
видань ДАК Міністерства освіти і науки України з технічних наук
(наказ №1021 від 07 жовтня 2015 р.)

Друкується згідно з рішенням вченої ради Кам'янець-Подільського
національного університету імені Івана Огієнка,
протокол № 6 від 23 травня 2019 року.

Рецензенти:

І. В. Бейко, доктор технічних наук, професор,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»;

Р. Н. Квстний, доктор технічних наук, професор, завідувач кафедри
Вінницького національного технічного університету.

Редакційна колегія:

О. М. Хіміч, член-кореспондент НАНУ,
доктор фізико-математичних наук, професор (*відповідальний редактор*);

А. Ф. Верлань, член-кореспондент НАПНУ,
доктор технічних наук, професор (*заст. відповідального редактора*);

В. А. Федорчук, доктор технічних наук, професор (*відповідальний секретар*);

Т. Бокалруд, доктор філософії, професор, Норвегія;

В. П. Боюн, член-кореспондент НАНУ, доктор технічних наук, професор;

В. В. Васильєв, член-кореспондент НАНУ, доктор технічних наук, професор;

А. А. Верлань, доктор філософії, професор, Норвегія;

В. К. Задірака, академік НАНУ, доктор фізико-математичних наук, професор;

І. М. Конет, доктор фізико-математичних наук, професор;

Б. Б. Нестеренко, доктор технічних наук, професор;

С. А. Положанко, доктор технічних наук, професор.

Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб.
М34 наук. праць / Інститут кібернетики імені В. М. Глушкова Національної
академії наук України, Кам'янець-Подільський національний університет
імені Івана Огієнка ; [редкол.: О. М. Хіміч (відп. ред.) та ін.]. — Кам'янець-
Подільський : Кам'янець-Подільський національний університет імені Івана
Огієнка, 2019. — Вип. 19. — 160 с.

У збірнику друкуються результати досліджень, що стосуються проблем
застосування математичних моделей у різних галузях людської діяльності.

Збірник включений до бази даних наукових журналів Норвегії.

Для наукових та інженерно-технічних працівників, докторантів, аспірантів,
студентів вищих навчальних закладів.

УДК 004.94:53.072
ББК 30

ISSN 2308-5916

DOI: 10.32626/2308-5916.2019-19

© Інститут кібернетики імені В. М. Глушкова НАН України, 2019

© Кам'янець-Подільський національний
університет імені Івана Огієнка, 2019

V. M. Glushkov Institute of Cybernetics
of National Academy of Sciences of Ukraine
Kamianets-Podilskyi National Ivan Ohiienko University

MATHEMATICAL AND COMPUTER MODELLING

Series: Technical sciences

Scientific journal

ISSUE 19

Kamianets-Podilskyi National Ivan Ohiienko University
2019

Critics:

I. Beyko, Doctor of Technical Science, Professor,
National Technical University of Ukraine

«Igor Sikorsky Kyiv Polytechnic Institute»;

R. Kvyetnyy, Doctor of Technical Science, Professor,
Head of department Vinnytsia national technical university.

Editorial board:

O. Himich, Corresponding Member of the NAS of Ukraine, Doctor
of Physical and Mathematical Sciences, Professor (*Executive Editor*);

A. F. Verlan, Corresponding Member of the NAPS of Ukraine,
Doctor of Technical Science, Professor (*Vice Executive Editor*);

V. Fedorchuk, Doctor of Technical Science,
Professor (*Responsible Secretary*);

T. Bokalrud, Associate Professor, Norway;

V. Boyun, Corresponding Member of the NAS of Ukraine,
Doctor of Technical Science, Professor;

I. Konet, Doctor of Physical and Mathematical Sciences, Professor;

B. Nesterenko, Doctor of Technical Science, Professor;

S. Polozhaenko, Doctor of Technical Science, Professor;

V. Vasiliev, Corresponding Member of the NAS of Ukraine,
Doctor of Technical Science, Professor;

A. A. Verlan, Ph. D., Professor, Norway;

V. Zadiraka, Academician of the NAS of Ukraine,
Doctor of Physical and Mathematical Sciences, Professor.

Mathematical and computer modelling. Series: Technical sciences: scientific journal / V. M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kamianets-Podilskyi National Ivan Ohiienko University ; [Editorial Board: O. Himich (Executive Editor) and others]. — Kamianets-Podilskyi : Kamianets-Podilskyi National Ivan Ohiienko University, 2019. — ISSUE 19. — 160 p.

The journal publishes results of studies on the mathematical models' application problems in various areas of human activity.

Joint with NTNU the journal has been included to the database of Norwegian Register for Scientific Journals, Series and Publishers.

Intended for scientific and engineering staff, researchers, undergraduate, graduate and Ph. D. students, post-graduates.

© V. M. Glushkov Institute of Cybernetics
of NAS of Ukraine, 2019

ISSN 2308-5916

DOI: 10.32626/2308-5916.2019-19

© Kamianets-Podilskyi National
Ivan Ohiienko University, 2019

Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам'янець-Подільський національний університет
імені Івана Огієнка

НАУКОВЕ ВИДАННЯ

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

Серія: Технічні науки

Збірник наукових праць

Випуск 19

Редактор **В. П. Замула**
Комп'ютерна верстка **О. М. Коломис**

Підписано до друку 20.06.2018 р. Гарнітура «Таймс».
Папір офсетний. Друк різнографічний.
Формат 60x84/16. Умовн. друк. арк. 9,3. Обл.-вид. арк. 10,1.
Тираж 100. Зам. № 862.

Кам'янець-Подільський національний університет імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

Надруковано в Кам'янець-Подільському національному
університеті імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

ЗМІСТ

Богаєнко В. А., Булавацький В. М., Гладкий А. В.
 Ідентифікація параметрів однієї дробово-диференціальної моделі міграції розчинних речовин..... 5

Bomba A. Ya., Voichura M. V.
 Numerical Complex Analysis Method for Parameters Identification of Anisotropic Media Using Applied Quasipotential Tomographic Data. Part 2: Algorithm and Numerical Experiment 11

Вакал Л. П., Вакал Є. С.
 Найкраще рівномірне наближення сплайнами з використанням диференціальної еволюції..... 17

Верлань А. Ф., Федорчук В. А., Іванюк В. А.
 Інтегральні моделі нестационарних задач теплопровідності на основі методу теплових потенціалів..... 24

Горбачук В. М., Дунаєвський М. С., Морозов О. О.
 Характеристики рівноваг ланцюгів постачання..... 31

Горбенко І. Д., Замула О. А., Хо Чи Лик
 Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно- комунікаційних системах..... 37

Горбенко Ю. І., Акользіна О. С., Подгайко В. О.
 Аналіз актуальних проблемних питань щодо перспективної асиметричної криптографії..... 44

Єсіна М. В.
 Моделі безпеки постквантових криптографічних примітивів..... 49

Корнієнко Б. Я., Галата Л. П.
 Оптимізація системи захисту інформації корпоративної мережі..... 56

Кудін А. М., Ковальчук Л. В., Коваленко Б. А.
 Теоретичні засади та застосування блокчейн-технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень 62

Кудряшов І. С., Малєєва Г. А.
 Аналіз властивостей електронних підписів на базі MQ-перетворень 69

Малачівський П. С., Монцібович Б. Р., Пізюр Я. В., Малачівський Р. П.
 Чебишовське наближення раціональним виразом функцій двох змінних 75

Матійко А. А. Порівняльний аналіз алгоритмів шифрування NTRUEncrypt та NTRUCipher	81
Мігін С. В. Застосування алгоритму bkw для відновлення систематичних лінійних блокових кодів за наборами спотворених кодових слів	88
Николайчук Л. М., Воронич А. Р., Заведюк Т. О. Методи нейропроцесорного опрацювання сигналів та комунікаційних взаємодій у середовищі суб'єктів права	94
Николайчук Я. М., Возна Н. Я., Грига В. М., Круліковський Б. Б., Давлетова А. Я. Високопродуктивні матричні та потокові перемножувачі цифрових даних	101
Огурцов М. І. Розробка протоколу захищеного обміну даними для спеціальних мереж	108
Олексійчук А. М., Конюшок С. М., Поремський М. В. Обґрунтування стійкості потокового шифру «Струмок» відносно кореляційних атак над скінченними полями характеристики 2.....	114
Онопрієнко В. В., Пономар В. А. Порівняльний аналіз постквантових асиметричних алгоритмів шифрування	120
Pankratov A., Romanova T. Decomposition Algorithm for Optimization Placement Problems.....	126
Пітух І. Р., Процюк Г. Я., Процюк В. Р. Алгоритми опрацювання моніторингових даних у діалогових системах	132
Шевчук Б. М. Підвищення інформаційної ефективності мереж та засобів інтернету речей	138
Якименко І. З., Касянчук М. М., Івасьєв С. В. Криптосистема Рабіна на основі операції додавання	145
Відомості про авторів	151
Алфавітний покажчик авторів	156