

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 15**

Кам'янець-Подільський національний університет  
імені Івана Огієнка  
2017

УДК 004.94:53.072

ББК 30

М34

Свідectво 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.)

Друкуються згідно з рішенням вченої ради Кам'янець-Подільського  
національного університету імені Івана Огієнка,  
протокол № 8 від 29 червня 2017 року.

#### Рецензенти:

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

**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. Положаєнко**, 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, 2017. — Вип. 15. — 272 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

© Інститут кібернетики імені В. М. Глушкова НАН України, 2017

© Кам'янець-Подільський національний  
університет імені Івана Огієнка, 2017

ISSN 2308-5916

V. M. Glushkov Institute of Cybernetics  
of National Academy of Sciences of Ukraine  
Kamianets-Podilsky National Ivan Ohienko University

# **MATHEMATICAL AND COMPUTER MODELLING**

**Series: Technical sciences**

Scientific journal

**ISSUE 15**

Kamianets-Podilsky National Ivan Ohienko University  
2017

### Critics:

**I. Beyko**, Doctor of Technical Science, Professor,  
National Technical University of Ukraine  
«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-Podilsky National Ivan Ohienko University ; [Editorial Board: O. Himich (Executive Editor) and others]. — Kamianets-Podilsky : Kamianets-Podilsky National Ivan Ohienko University, 2017. — ISSUE 15. — 272 p.

The book 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, 2017

© Kamianets-Podilsky National  
Ivan Ohienko University, 2017

ISSN 2308-5916

## ЗМІСТ

<b>Апарцин А. С., Маркова Е. В., Сидлер И. В., Труфанов В. В.</b> О поиске оптимальной стратегии развития электроэнергетической системы.....	5
<b>Бейко І. В., Щирба О. В.</b> Методи оптимізації узагальнених динамічних моделей В. М. Глушкова.....	11
<b>Белецкий А. Я.</b> Уолша-подобные системы секвентных функций.....	17
<b>Вакал Л. П., Вакал Є. С.</b> Розв'язання перевизначеної системи трансцендентних рівнянь з використанням диференціальної еволюції.....	24
<b>Верлань А. Ф., Махович О. І.</b> Підхід до вибору опорних перерізів в інтерполяційному методі редукції моделей об'єктів із розподіленими параметрами.....	30
<b>Verlan A., Fedorchuk V.</b> On the Choice of Numerical Methods for Solving Dynamic Equations for Control Systems with Embedded Calculating Tools .....	37
<b>Ганзя Р. С.</b> Модифікований метод обчислення порядку еліптичних кривих.....	43
<b>Гибкіна Н. В., Сидоров М. В., Стороженко О. В.</b> Економетричний аналіз показників інфляції в Україні за даними 2000–2015 років .....	49
<b>Горбачук В. М., Морозов О. О., Неботов П. Г.</b> Моделі поведінки фірм ринку природного газу.....	55
<b>Іванюк В. А., Дячук О. А., Понеділок В. В.</b> Метод обернених операторів відновлення сигналів на вході лінійних динамічних систем, що задані передатними функціями.....	62
<b>Карпець Е. П., Кузьменко В. М.</b> Загальний алгоритм визначення впливу економічних зрушень на базі балансних моделей.....	67
<b>Касянчук М. М., Якименко І. З., Івасьєв С. В., Масляк Б. О.</b> Метод розширення набору модулів модифікованої досконалої форми системи залишкових класів .....	73
<b>Качко О. Г., Макутоніна Л. В., Акользіна О. С.</b> Оптимізація NTRU подібного алгоритму для несиметричного шифрування з «незручними параметрами» .....	79
<b>Корнієнко Б. Я.</b> Аналіз математичних моделей процесів зневоднення та гранулювання у псевдозрідженому шарі.....	86
<b>Котух Є. В.</b> Асимптотичні оцінки універсального хешування за алгебричними кривими.....	92

<b>Круліковський Б. Б., Возна Н. Я., Грига В. М., Давлетова А. Я.</b> Оптимізація структурних рішень комбінаційних суматорів згідно критеріїв мінімальної часової, апаратної та структурної складності .....	97
<b>Кудин А. М.</b> Блокчейн и криптовалюты на основании «доказательства точности» ...	104
<b>Кузнецов О. О., Пушкарьов А. І., Горбенко Ю. І.</b> Кодові криптосистеми для постквантового застосування .....	109
<b>Лисицький К. Є.</b> Оптимізація перспективних алгоритмів симетричного блочного перетворення по критеріям швидкодії і стійкості .....	115
<b>Маслова Н. О.</b> Застосування задачі розподілу ресурсів в системах захисту інформації .....	120
<b>Мельникова О. А., Масленнікова А. О.</b> Підстановки для підвищення ефективності програмної реалізації алгоритмів, які використовують знаково-цифрові представлення ...	126
<b>Мосенцова Л. В.</b> Численно-аналитический алгоритм интерпретации в задаче восстановления сигнала .....	132
<b>Николайчук Л. М., Вирховська А. Т.</b> Інформаційні моделі оператора комп'ютеризованої системи як суб'єкта права .....	138
<b>Николайчук Я. М., Волинський О. І., Гуменний П. В., Пастух Т. І.</b> Методи міжбазисних перетворень багаторозрядних кодів теоретико-числових базисів Радемахера – Крестенсона .....	143
<b>Олексійчук А. М., Ігнатенко С. М., Поремський М. В.</b> Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями .....	150
<b>Олійник Г. В., Грибков С. В.</b> Модифікований АСО алгоритм побудови календарного плану виконання договорів .....	156
<b>Перекопський О. О.</b> Порівняльний аналіз доказу виконаної роботи та візантійської відмовостійкості .....	162
<b>Першина Ю. І., Шилін О. В.</b> Метод відновлення 3D об'єкта з використанням поліноміальної інтерфлетачії .....	167
<b>Пітух І. Р., Процюк Г. Я., Процюк В. Р., Албанський І. Б.</b> Система автоматизованого проектування інтерактивної взаємодії оператора комп'ютеризованого керування багатопараметричним об'єктом на основі образно-кластерної моделі .....	173
<b>Полуяненко Н. А.</b> Расчет числа образующих полиномов для регистров сдвига с нелинейной обратной связью с нелинейностью произвольного порядка .....	179

<b>Пономар В. А.</b> Стан, методика та проміжні підсумки розробки проектів постквантових криптографічних примітивів.....	185
<b>Потій О. В., Ісірова К. В.</b> Аналіз вимог та моделей безпеки для постквантової криптографії....	192
<b>Ревенчук І. А.</b> Математична модель агрегації даних в соціальних медіа.....	197
<b>Родінко М. Ю.</b> Малоресурсний симетричний блоковий шифр «Кипарис» — сутність та основні властивості.....	203
<b>Сабадаш І. О., Люра О. П.</b> Алгоритм опрацювання даних та компоненти спецпроцесора релейного захисту високовольтних ліній електропересилань.....	209
<b>Сегін А. І.</b> Визначення оцінки сумарного кореляційного взаємовпливу періодичних процесів з багатократним повторенням та представленням в полярній системі координат.....	215
<b>Солодуша С. В.</b> К идентификации ядер Вольтерры в нестационарных интегральных моделях динамических систем.....	222
<b>Sterten Jo, Furtat Yu. O.</b> Regularized Methods of Noisy Signals Differentiation in Real Time.....	228
<b>Стеценко П. І.</b> Масштабні атаки на децентралізовані системи, що побудовані на однорангових пірингових мережах.....	233
<b>Теліженко О. Б.</b> Структура групи точок кривої Едвардса, що не містить точок восьмого порядку.....	239
<b>Трембач Р. Б., Трембач Б. Р., Сидор А. І., Возна Г. В.</b> Структура та системні характеристики спецпроцесорів визначення Хеммінгової віддалі реалізованих в різних теоретико-числових базисах.....	244
<b>Халімов Г. З.</b> Аналіз складності реалізацій криптосистем на групах.....	250
<b>Шевчук Б. М.</b> Завадостійка передача захищених пакетів даних в інформаційно-ефективних радіомережах.....	255
<b>Відомості про авторів</b> .....	262
<b>Алфавітний покажчик авторів</b> .....	267