КІБЕРНЕТИКА **CYBERNETICS**

УДК 004.8

Глобальні тренди штучного інтелекту: виклики, можливості, перспективи / М.З. Згуровський // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 9–31.

Анотація. Феномен стрімкої трансформації світу під впливом штучного інтелекту (ШІ) зумовлений його здатністю прискорювати інновації, змінювати економічні процеси, впливати на способи взаємодії людей із технологіями та відкривати нові перспективи для розвитку людства. Останні роки характеризуються безпрецедентним темпом впровадження ШІ у ключові сфери життя, що суттєво змінює ринок праці, наукові дослідження, соці- альні комунікації, глобальну безпеку та економіку. Проте ці зміни потребують усвідомленого підходу до регулювання, визначення етичних меж та адаптації суспільства до нових технологічних реалій. Важливо, щоб ШІ залишався інструментом прогресу, що сприяє сталому розвитку, а не створював загрозу для стабільності та добробуту людства.

Ключові слова: штучні нейронні мережі, дата-центри, графічні процесори (GPU), тензорні процесори (TPU), нейронні процесори (NPU), великі дані (Big Data), машинне навчання, оброблення природної мови (NLP), сценарії розвитку ШІ.

Global Trends in artificial intelligence: Challenges, opportunities, and prospects / M.Z. Zgurovsky // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 9–31.

Abstract. The phenomenon of the rapid transformation of the world under the influence of artificial intelligence (AI) is driven by its ability to accelerate innovation, reshape economic processes, influence the ways people interact with technology, and open new perspectives for human development. In recent years, AI has been integrated into key areas of life at an unprecedented pace, significantly transforming the labor market, scientific research, social communications, global security, and the economy. However, these changes require a conscious approach to regulation, the establishment of ethical boundaries, and the adaptation of society to new technological realities. It is crucial to ensure that AI remains a tool for progress, fostering sustainable development rather than posing a threat to stability and human well-being.

Keywords: artificial neural networks, data centers, graphics processing units (GPU), tensor processing units (TPU), neural processing units (NPU), big data, machine learning, natural language processing (NLP), AI development scenarios.

==========

СИСТЕМНИЙ АНАЛІЗ **SYSTEMS ANALYSIS**

УДК 519.64:517.443:519.254

Елементи загальної теорії оптимальних алгоритмів / В.К. Задірака, І.В. Швідченко // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 32–45.

Анотація. Наведено загальну схему оцінки повної похибки обчислювального алгоритму. Побудовано оптимальні алгоритми за умов найбільш повного використання наявної інформації про задачу. Розглянуто резерви оптимізації обчислень.

Ключові слова: обчислювальний алгоритм, наближений розв'язок, похибка наближеного розв'язку, оптимізація алгоритмів, резерви оптимізації обчислень, комп'ютерні технології.

Elements of the general theory of optimal algorithms / V.K. Zadiraka, I.V. Shvidchenko // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 32–45.

Abstract. A general scheme for estimating the total error of a computational algorithm is presented. Optimal algorithms are constructed under the conditions of the most complete use of available information about the problem. Reserves for optimization of calculations are considered.

Keywords: computational algorithm, approximate solution, error of approximate solution, optimization of algorithms, reserves of calculations optimization, computer technologies.

==========

УДК 621.391:519.2:519.7

Застосування загальної теорії оптимальних алгоритмів у криптографії, стеганографії та блокчейн-технології / А.М. Кудін, І.А. Кудін, В.З. Чіхладзе // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 46–57.

Анотація. Аналіз та синтез односторонніх функцій та односторонніх функцій з лазів- кою є основою для оцінювання стійкості та побудови криптографічних перетворень, стеганографічних систем та протоколів консенсусу блокчейнів. Розглянуто інформаційно- обчислювальний підхід до побудови таких функцій на основі загальної теорії оптимальних алгоритів та їхнє застосування в криптографії, стеганографії, аналізі та синтезі протоколів консенсусу блокчейнів.

Ключові слова: загальна теорія оптимальних алгоритмів, односторонні функції, односторонні функції з лазівкою, оцінки стійкості криптосистем, стеганографія, блокчейн.

Application of the general theory of optimal algorithms in cryptography, steganography, and blockchain technology / A.M. Kudin, I.A. Kudin, V.Z. Chikhladze // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 46–57.

Abstract. Analysis and synthesis of one-way and trapdoor functions are the basis for security estimates and the construction of cryptographic transformations, steganographic systems, and blockchain consensus protocols. The paper considers the information-computational approach to creating such functions based on the general theory of optimal algorithms and their applications in cryptography, steganography, and the analysis and synthesis of blockchain consensus protocols.

Keywords: a general theory of optimal algorithms, one-way function, trapdoor function, cryptosystem's security estimates, steganography, blockchain.

==========

УДК 519.65

Чебишовське наближення функцій багатьох змінних нелінійною функцією від раціонального виразу / П.С. Малачівський, Л.С. Мельничок // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 58–69.

Анотація. Запропоновано метод побудови чебишовського наближення функцій багатьох змінних експонентою, логарифмом і фіксованим дійсним степенем від раціонального виразу. Він полягає в побудові проміжного чебишовського наближення раціональним виразом відповідного функціонального перетворення наближуваної функції. Наближення раціональним виразом обчислено як граничне середньостепеневе наближення за ітераційною схемою з використанням методу найменших квадратів з двома змінними ваговими функціями. Наведено тестові приклади, які підтверджують швидку збіжність методу.

Ключові слова: чебишовське наближення, функції багатьох змінних, раціональний вираз, середньостепеневе наближення, наближення нелінійними виразами, метод найменших квадратів.

Chebyshev approximation of multivariable functions by a nonlinear function of a rational expression / P.S. Malachivskyy, L.S. Melnychok // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 58–69.

Abstract. A method for constructing Chebyshev approximations of multivariable functions using an expression that is an exponent, a logarithm, or a fixed real power from a rational expression is proposed. It involves constructing an intermediate Chebyshev approximation by a rational expression of the corresponding functional transformation of the approximated function. The approximation by a rational expression is calculated as a limiting mean-power approximation by an iterative scheme using the least squares method with two variable weight functions. Test examples are provided that confirm the fast convergence of the method.

Keywords: Chebyshev approximation, multivariable function, rational expression, approximation by nonlinear expressions, mean-power approximation, least squares method.

==========

УДК 519.6

Наближене обчислення подвійних інтегралів від швидкоосцилювальних функцій загального вигляду з використанням оптимальної за порядком точності кубатурної формули на класі диференційовних функцій / О.П. Нечуйвітер // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 70–76.

Анотація. Розглянуто задачу наближеного обчислення подвійних інтегралів від швидкоосцилювальних функцій загального вигляду (іррегулярний випадок). Побудовано кубатурну формулу, яка використовує інформаційні оператори О.М. Литвина та кусково-лінійні сплайни як допоміжні функції. Інформація про функції задається відповідними значеннями на лініях. Доведено, що запропонована кубатурна формула є оптимальною за порядком точності на класі дифренційовних функцій.

Ключові слова: оптимальне чисельне інтегрування, швидкоосцилювальні функції загального вигдяду, інформаційні оператори, оптимальна за порядком точності квадратурна формула, диференційовні функції двох змінних.

Approximate calculation of double integrals of highly oscillating functions of general type using the cubature formula of optimal order of accuracy on a class of differentiable functions / O.P. Nechuiviter // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 70–76.

Abstract. The problem of approximating double integrals of highly oscillating functions of general type (irregular case) is considered. A cubature formula is constructed that uses O.M. Lytvyn's information operators and piecewise linear splines as auxiliary functions. Information about the functions is provided by the corresponding values on the lines. It is proved that the proposed cubature formula is optimal in order of accuracy on the class of differentiable functions.

Keywords: optimal numerical integration, highly oscillating functions of general type, O.M. Lytvyn's information operators, cubature formula optimal in order of accuracy, differential functions of two variables.

==========

УДК 519.6:517.524

Розв'язування матричних поліноміальних рівнянь / М.О. Недашковський // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 77–93.

Анотація. Матричні рівняння та системи матричних рівнянь широко використовують у задачах оптимізації систем управління, в математичній економіці. Однак методи їхніх розв'язувань сформовані лише для найбільш поширених матричних рівнянь — рівнянь Ріккаті та Ляпунова, а універсального підходу до розв'язання задач такого класу не існує. У цій роботі розглянуто методи розв'язання матричних поліноміальних рівнянь довільного порядку з матричними та векторними невідомими. Описано підхід до обчислення кортежів розв'язків поліноміальних матричних рівнянь, який базується на теорії гіллястих ланцюгових дробів. Зазначимо, що йдеться не лише про чисельні, а й про символьні методи розв'язання. Подано обчислювальну схему для систем поліноміальних матричних рівнянь другого степеня з багатьма невідомими. Наведено розвинення розв'язку у неперервний ланцюговий матричний дріб. Сформульовано достатні ознаки збіжності матричних гіллястих ланцюгових дробів до розв'язків та критерії закінчення обчислень в ітераційних операціях. Результати чисельних експериментів підтверджують справедливість теоретичних викладок та ефективність запропонованих методів.

Ключові слова: матричні поліноміальні рівняння, гіллясті ланцюгові дроби з матричними елементами, збіжність до розв'язку.

Solving matrix polynomial equations / M. Nedashkovskyy // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 77–93.

Abstract. Matrix equations and systems of matrix equations are widely used in problems of optimization of control systems, in mathematical economics. However, methods for solving them are developed only for the most popular matrix equations – the Riccati and Lyapunov equations, and there is no universal approach to solving problems of this class. This paper discusses methods for solving matrix polynomial equations of arbitrary order with matrix and vector unknowns. An approach to calculating tuples of solutions of polynomial matrix equations, which is based on the theory of branched chain fractions, is given. It should be noted that we are talking not only about numerical but also symbolic methods of solution. The paper also presents a computational scheme for systems of second-degree polynomial matrix equations with many unknowns. The solution is developed into a continued matrix fraction. Sufficient signs of convergence of branched continued matrix fractions to the solutions and the criteria for completing calculations in iterative procedures are formulated. The results of numerical experiments are presented, confirming the validity of the theoretical calculations and the effectiveness of the proposed methods.

Keywords: matrix polynomial equations, branched continued fractions with matrix elements, convergence to solution.

==========

УДК 519.85

Наукова спадщина академіка Н.З. Шора / П.І. Стецюк // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 94–103.

Анотація. Наведено огляд наукової спадщини академіка Н.З. Шора. Розглянуто його основні наукові ідеї: метод послідовного аналізу варіантів (1961 р.), субградієнтний метод (1962 р.), використання лінійних неортогональних перетворень простору для покращення обумовленості яружних функцій (1969 р.), двоїстий підхід до отримання та уточнення оцінок цільової функції у неопуклих квадратичних моделях (1985 р.). Наведено приклади втілення цих ідей у методах та алгоритмах, розроблених в Інституті кібернетики ім. В.М. Глушкова НАН України.

Ключові слова: негладка (недиференційовна) функція, субградієнтний метод, оператор розтягу простору, метод еліпсоїдів, -алгоритм, квадратична екстремальна задача.

The scientific heritage of academician Shor / P.I. Stetsyuk // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 94–103.

Abstract. An overview of the scientific heritage of Academician N.Z. Shor is provided. His fundamental scientific ideas are considered, including the method of sequential analysis of variants (1961), subgradient method (1962), the use of linear non-orthogonal space transformations for improving the properties of ravine functions (1969), and a dual approach for obtaining and refining objective function estimates in non-convex quadratic models (1985). Examples of implementing these ideas in the methods and algorithms developed at the V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine are presented.

Keywords: non-smooth (non-differentiable) function, subgradient method, space dilation operator, ellipsoid method, *r*-algorithm, extremal quadratic problem.

==========

УДК 517.988

Метод операторної екстраполяції для варіаційних нерівностей та його застосування / В.В. Семенов // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 104–117.

Анотація. Досліджено нові ітераційні алгоритми для розв'язання монотонних варіаційних нерівностей у Гільбертовому просторі. Запропоновано варіант алгоритму операторної екстраполяції зі змінною метрикою. Доведено теореми про слабку та сильну збіжність для варіаційних нерівностей з Ліпшицевими та монотонними операторами. Розглянуто декілька застосувань алгоритму операторної екстраполяції для задач сідлового типу.

Ключові слова: варіаційна нерівність, сідлова задача, рівновага Неша, операторне рівняння, метод операторної екстраполяції, метод змінної метрики, збіжність.

The operator extrapolation method for variational inequalities and its application / V.V. Semenov // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 104–117.

Abstract. The study focuses on new iterative algorithms for solving monotone variational inequalities in Hilbert space. A variant of the operator extrapolation algorithm with a variable metric is proposed. Theorems on weak and strong convergence for variational inequalities with Lipschitz continuous and monotone operators are proved. Several applications of the operator extrapolation algorithm for saddle-type problems are considered.

Keywords: variational inequality, saddle point problem, Nash equilibrium, operator equation, operator extrapolation method, variable metric method, convergence.

==========

УДК 621.396

Методи, алгоритми та засоби дистанційного тривалого моніторингу стану безпеки людей та об'єктів їхньої власності / Б.М. Шевчук // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 118–133.

Анотація. Запропоновано методологічні та алгоритмічні основи функціонування терміналь- них, локально-регіональних та глобальних безпровідних мереж тривалого моніторингу стану безпеки великої кількості людей та об'єктів їхньої власності. З урахуванням роботи портативних об'єктних систем моніторингової мережі з багатьма обмеженнями запропоновано оперативне оброблення і кодування вибірок моніторингових сигналів і кадрів відеоданих. Кодування введених моніторингових даних від давачів, сенсорів і відеомодулів здійс- нюється на основі сигнального підходу. Згідно з цим підходом процесорними засобами об'єктних систем у процесі фільтрації та стиску моніторингових сигналів і зображень забезпечується точне кодування, декодування та відновлення параметрів найбільш інформативних відліків сигналів та пікселів відеосигналів, до яких належать екстремуми і точки перегину обвідних сигналів і відеосигналів. Захист масивів моніторингових даних запропоновано здійснювати в процесі стиску та захисту даних з використанням одноразових шиф- рів. Розглянуто побудову енергоефективних та високоінформативних портативних об'єкт- них систем тривалого моніторингу мешканців міст і сіл, операторів людино-машинних систем і комплексів, рухомих і нерухомих об'єктів.

Ключові слова: методи та алгоритми моніторингу стану безпеки людей, моніторингові радіомережі, об'єктні системи, оброблення, кодування та передавання сигналів і зображень, стиск та захист даних моніторингу, одноразові шифри, криптопослідовності.

Methods, algorithms, and tools for remote long-term monitoring of the safety of people and their property / B.M. Shevchuk // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 118–133.

Abstract. The methodological and algorithmic foundations of the functioning of terminal, local-regional, and global wireless networks for long-term security monitoring of large groups of people and their property are proposed. Taking into account the operation of portable object systems of the monitoring network with many limitations, the operational processing and encoding of samples of monitoring signals and video data frames are proposed. The input monitoring data from sensors, transducers, and video modules is encoded based on the signal approach. According to this approach, the processing means of object systems in the process of filtering and compressing monitoring signals and images ensure accurate encoding, decoding, and restoration of the parameters of the most informative signal samples and video signal pixels, which include extrema and inflection points of the contour signals and video signals. It is proposed to protect the monitoring data arrays during the compression process with data protection using one-time ciphers. The article focuses on constructing energy-efficient and highly informative portable object systems for long-term monitoring of urban and rural residents, operators of human-machine systems and complexes, as well as mobile and stationary objects.

Keywords: methods and algorithms for monitoring human safety, monitoring radio networks, object systems, processing, encoding and transmission of signals and images, compression and protection of monitoring data, one-time ciphers, crypto sequences.

==========

УДК 621.391:519.2:519.7

Моделювання спрощеного варіанта атаки розгалуження на блокчейн, ґрунтований на протоколі консенсусу Proof-of-Stake / Л.В. Ковальчук, М.Ю. Кузнєцов, А.А. Шумська // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 134–145.

Анотація. Відомо, що атака розгалуження є однією з найважливіших атак на блокчейн, насамперед для протоколів Proof-of-Work та Proof-of-Stake, як найбільш поширених. На сьогодні немає явних аналітичних формул для обчислення ймовірності її успіху, що викликає певну недовіру до блокчейн-технологій. У цій роботі для спрощеної (але все одно достатньо складної з математичного погляду) моделі атаки розгалуження отримано рекурентні формули, які дають змогу знаходити точні значення ймовірності того, що зловмисник зможе побудувати розгалуження заданої довжини. Коректність цих формул перевіряється на числових прикладах методом Монте-Карло шляхом побудови оцінок із заданими достовірністю та відносною похибкою.

Ключові слова: блокчейн, Proof-of-Stake, атака розгалуження, стейкхолдер, таймслот, слотлідер, рекурентні формули, метод Монте-Карло.

Simulating a simplified version of a splitting attack on the blockchain based on the Proof-of-Stake consensus protocol / L.V. Kovalchuk, M.Yu. Kuznetsov, A.A. Shumska // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 134–145.

Abstract. The splitting attack is one of the most important attacks on the blockchain, first of all for Proof-of-Work and Proof-of-Stake consensus protocols. Currently, there are no explicit analytical formulas for evaluating its success probability, which causes some distrust in blockchain technologies. In this paper, for a simplified (but still not simple) model of a splitting attack, the recurrent formulas allowing the evaluation of the exact values of the probability that an attacker will be able to build a branch of a given length are obtained. The correctness of these formulas is verified through numerical examples using the Monte Carlo method by constructing estimates with a specified confidence level and relative error.

Keywords: blockchain, Proof-of-Stake, splitting attack, stakeholder, timeslot, slotleader, recursive formulas, Monte Carlo method.

==========

НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ І СИСТЕМНОГО АНАЛІЗУ

NEW TOOLS IN CYBERNETICS, COMPUTER SCIENCE, AND SYSTEM ANALYSIS

УДК: 004.056.5

Національні та міжнародні постквантові стандарти асиметричних перетворень / І.Д. Горбенко, С.О. Кандій // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 146–159.

Анотація. Проаналізовано сучасний стан та перспективи стандартизації постквантових алгоритмів асиметричних криптографічних перетворень на національному та міжнародному рівнях. Розглянуто основні причини переходу до постквантової криптографії, зокрема потенційні загрози з боку квантових комп'ютерів наявним криптографічним алгоритмам (RSA, ECC тощо). Наведено огляд конкурсу NIST з вибору стандартів для постквантових механізмів інкапсуляції ключів (KEM) та електронного підпису, а також детально описано алгоритми, вибрані для стандартизації (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+ та HQC). Проаналізовано роль організацій ISO/IEC, ETSI, а також групи IETF у формуванні міжнародних стандартів та рекомендацій. Окрему увагу приділено українським національним стандартам та ініціативам, зокрема алгоритмам «Скеля» та «Вершина», їхнім особливостям та перспективам інтеграції у міжнародні стандарти. Стаття дає розуміння важливості та складності процесу переходу до квантово-стійких алгоритмів й окреслює подальші кроки для успішного впровадження постквантової криптографії.

Ключові слова: постквантова криптографія, механізми інкапсуляції ключів, електронні підписи, стандартизація.

National and international post-quantum standards for asymmetric transformations / I.D. Gorbenko, S.O. Kandii // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 146–159.

Abstract. The article analyzes the current state and prospects of the standardization of post-quantum algorithms for asymmetric cryptographic transformations at the national and international levels. The main reasons for the transition to post-quantum cryptography are discussed, particularly the potential threats posed by quantum computers to existing cryptographic algorithms (RSA, ECC, etc.). An overview of the NIST competition for selecting standards for post-quantum key encapsulation mechanisms (KEM) and electronic signatures is provided, with detailed descriptions of the algorithms chosen for standardization (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+, and HQC). Additionally, the article examines the role of ISO/IEC, ETSI, and IETF in developing international standards and recommendations. Special attention is given to Ukrainian national standards and initiatives, particularly the algorithms "Skelya" and "Vershyna," their features, and their prospects for integration into international standards. The article emphasizes the importance and complexity of transitioning to quantum-resistant algorithms and outlines further steps for the successful implementation of post-quantum cryptography.

Keywords: post-quantum cryptography, key encapsulation mechanisms, electronic signatures, standardization.

УДК 003.26:621.39+530.145

Сучасні квантові технології криптографічного захисту інформації / Є.В. Васіліу // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 160–175.

Анотація. Квантова криптографія являє собою нову парадигму криптографічного захисту інформації з використанням законів квантової механіки та відповідних квантових властивостей носіїв інформації — фотонів для усунення обмежень класичних криптографічних протоколів та підвищення стійкості криптопротоколів аж до теоретико-інформаційного рівня. У роботі наведено загальний огляд та аналіз сучасних квантових технологій захисту інформації, зокрема протоколів квантового розподілення ключів, квантового прямого безпечного зв'язку, квантового розділення секрету. Стисло розглянуто декілька інших напрямів квантової криптографії, як-от квантовий цифровий підпис, квантове бітове зобов'язання, квантова стеганографія тощо. Проаналізовано переваги та недоліки протоколів квантової криптографії, перспективи та проблеми їхнього практичного впровадження. Надано короткий огляд законів квантової фізики, на яких ґрунтується стійкість протоколів квантової криптографії.

Ключові слова: квантова криптографія, фізичні основи квантової криптографії, кубіт, кудит, переплутані кубіти та кудити, квантове розподілення ключів, квантовий прямий безпечний зв'язок, квантове розділення секрету.

Modern quantum technologies of cryptographic information protection / Ye. Vasiliu // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 160–175.

Abstract. Quantum cryptography is a new paradigm of cryptographic information protection, utilizing the laws of quantum mechanics and the corresponding quantum properties of information carriers — photons to overcome the limitations of classical cryptographic protocols and increase the security of cryptographic protocols up to the information-theoretic level. The paper provides a general overview and analysis of modern quantum information security technologies, particularly protocols for quantum key distribution, quantum secure direct communication, and quantum secret sharing. Several other areas of quantum cryptography are briefly considered, such as quantum digital signature, quantum bit commitment, quantum steganography, etc. The advantages and disadvantages of quantum cryptographic protocols, as well as the prospects and challenges of their practical implementation, are analyzed. A brief overview of the laws of quantum physics underlying the security of quantum cryptographic protocols is also provided.

Keywords: quantum cryptography, physical foundations of quantum cryptography, qubit, qudit, entangled qubits and qudits, quantum key distribution, quantum secure direct communication, quantum secret sharing.

==========

УДК 621.396

Високопродуктивні обчислення в системі класів лишків / Я.М. Николайчук, І.Р. Пітух // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 176–189.

Анотація. Наведено математичні основи кодування даних та виконання модульних операцій у системі класів лишків (СКЛ). Досліджено математичні перетворення системи ортогональних гармонічних функцій теоретико-числового базису Фур'є. Побудовано моделі формування кодів СКЛ на основі фазових портретів гармонічних функцій, частоти яких відповідають умовам взаємної простоти. Розглянуто моделі формування дискретно-квантованих пилкоподібних функцій фазових портретів гармонічних частот у системі модулів класів лишків , , . Наведено алгоритми формування та опрацювання цифрових даних, поданих кодами найменших невід'ємних лишків. Проаналізовано алгоритми виконання обчислювальних операцій у кодах цілочислової, нормалізованої та досконалої форм СКЛ. Запропоновано методи та алгоритми виконання високопродуктивних арифметико-логічних операцій у кодах СКЛ. Досліджено характеристики швидкодії виконання арифметико-логічних операцій у СКЛ цифрових даних, представлених у теоретико-числових базисах Радемахера, Радемахера–Крестенсона та Хаара–Крестенсона. Проаналізовано алгоритми порівняння чисел у кодах СКЛ. Досліджено методи формування кодів лишків на основі аналогових та цифрових даних. Розроблено метод перетворення двійкових кодів теоретико-числового базису Радемахера у коди лишків за модулем у СКЛ. Побудовано алгоритм визначення вибіркового математичного сподівання в СКЛ на основі визначення суми рангів потокового опрацювання даних. Досліджено метод перетворення представлених у СКЛ багаторозрядних чисел у двійкові коди теоретико-числового базису Радемахера. Наведено структури спецпроцесорів, які реалізують обчислювальні задачі у СКЛ.

Ключові слова: гармонічні функції Фур'є, система класів лишків, алгоритми, високопродуктивні обчислення, функціональні схеми спецпроцесорів.

High-performance computing in the residual class system / Y. Nikolaychuk, I. Pitukh // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 176–189.

Abstract. The mathematical foundations of data coding and performing modular operations in the residual class system are outlined. The mathematical transformations of the system of orthogonal harmonic functions of the Fourier number-theoretic basis are investigated. Models of forming codes of the residual class system are constructed based on phase portraits of harmonic functions, the frequencies of which meet the conditions of mutual simplicity. Models of forming discrete-quantized sawtooth functions of phase portraits of harmonic frequencies in the residual class module system are presented. Algorithms for forming and processing digital data represented by codes of the smallest non-negative residues are investigated. Algorithms for performing computational operations in codes of integer, normalized, and perfect forms of the residual class

system are analyzed. Methods and algorithms for performing high-performance arithmetic and logical operations in codes of the residual class system are proposed. The characteristics of the speed of performing arithmetic and logical operations in the system of residual classes of digital data represented in the Rademacher, Rademacher–Krestenson, and Haar–Krestenson number-theoretic bases are studied. The algorithms for comparing numbers in the codes of the residual class system are analyzed. The methods for forming residue codes based on analog and digital data are studied. A method for converting binary codes of the Rademacher number-theoretic basis into residue codes modulo the residual class system is developed. An algorithm for determining the sample mathematical expectation in the residual class system based on determining the sum of ranks of streaming data processing is presented. A method for converting multi-digit numbers represented in the residual class system into binary codes of the Rademacher number-theoretic basis is studied. The structures of special processors that implement computational tasks in the residual class system are presented.

Keywords: Fourier harmonic functions, residual class system, algorithms, high-performance computing, functional diagrams of special processors.

==========

УДК 004.93+621.396

Застосування методів машинного навчання до деяких проблем цифрового оброблення сигналів у телекомунікаційних задачах / В.Ю. Семенов, Є.В. Семенова // Кібернетика та системний аналіз. 2025. Том 61, № 4. С. 190–198.

Анотація. Розглянуто застосування методів машинного навчання до задач цифрового оброблення сигналів у телекомунікаційних системах, зокрема, задач автоматичної класифі- кації модуляції та подальшої демодуляції сигналу. Для автоматичної класифікації модуляції досліджено чотири методи машинного навчання: мультиноміальну регресію, метод найближчих сусідів, метод гауссівських сумішей та згорткову нейронну мережу. Експериментальні результати на штучних даних показали точність розпізнавання п'яти класів модуляції на рівні від 96 % до 99 %. Найвищу точність (99 %) забезпечила згорткова нейронна мережа. Проте три інші методи, що мають простішу структуру, демонструють задовільний компроміс між точністю та складністю реалізації. Перевірка на 89 сигналах від реальних модемів показала, що метод найближчих сусідів досягає найвищої точності класифікації (100 %), тоді як решта методів забезпечують точність на рівні 99 %. Це свідчить про те, що висока точність класифікації може бути досягнута за допомогою значно простіших методів порівняно із згортковими нейронними мережами. Запропоновано метод блокової демодуляції сигналів на основі мультиноміальної лінійної регресії та нейронної мережі прямого зв'язку, що має просту практичну реалізацію порівняно з іншими відомими методами. Показано, що у разі високих рівнів шуму запропонований метод забезпечує вищу точність відновлення сигналу порівняно з традиційним методом демодуляції на основі контурів Гарднера та Костаса, а також використовує меншу кількість параметрів ніж інші відомі методи.

Ключові слова: машинне навчання, глибоке навчання, цифрове оброблення сигналів, автоматична класифікація модуляції, демодуляція сигналів.

Application of machine learning methods to certain problems of digital signal processing in telecommunication tasks / V.Yu. Semenov, E.V. Semenova // Kibernetyka ta Systemnyi Analiz. 2025. Vol. 61, N 4. P. 190–198.

Abstract. The article explores the application of machine learning methods to digital signal processing tasks in telecommunication systems. Specifically, it examines the problems of automatic modulation classification and subsequent signal demodulation. For automatic modulation classification, four machine learning methods are investigated: multinomial regression, nearest neighbors' method, Gaussian mixture modeling, and a convolutional neural network. Experimental results on artificial data demonstrated recognition accuracy for five modulation types ranging from 96% to 99%. The highest accuracy (99%) was achieved by the convolutional neural network. However, the three other methods, which have a simpler structure (and were not considered in previous works), show a satisfactory trade-off between accuracy and implementation complexity. Verification on 89 signals from real modems showed that the nearest neighbors' method achieves the highest classification accuracy (100%), while the remaining methods provide accuracy at the level of 99%. This indicates that high classification accuracy can be achieved using significantly simpler methods compared to convolutional neural networks. The paper also proposes a method of block demodulation of signals based on multinomial linear regression and a feedforward neural network, which has a simpler practical implementation compared to other known methods. It is shown that at high noise levels, the proposed method provides higher signal recovery accuracy compared to the traditional demodulation method based on Gardner and Costas loops, and also uses fewer parameters compared to other known methods.

Keywords: machine learning, deep learning, digital signal processing, automatic modulation classification, signal demodulation.

==========