КІБЕРНЕТИКА **CYBERNETICS**

УДК 004.93.12

Визначення центроїда лазерної плями у площині фотосенсора мультимедійного тиру на основі методів інтерполяції та фільтрації фрагмента зображення / С.В. Яременко, Ю.В. Крак // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 3–11.

Анотація. Розглянуто задачу визначення центроїда проєкції лазерної плями на площині фотосенсора у мультимедійному тирі. Запропоновано двоетапний підхід до розв'язання цієї задачі. Досліджено можливості підвищення точності визначення центроїда за рахунок явного виділення контурів плями (другий етап оброблення) замість визначення країв плями з використанням порогової бінаризації. Проведено аналіз підходів до визначення країв плями. Для розв'язання задачі збільшено масштаб фрагмента зображення за рахунок інтерполяції нових точок. Досліджено можливості виділення контуру плями шляхом оброблення фрагмента зображення фільтрами низьких та високих частот. Проведено порівняльну оцінку точності базового алгоритму порівняно з модифікованим варіантом. Показано, що модифікований алгоритм забезпечує підвищення точності визначення центроїда на 30 %. Підвищення точності досягнуто завдяки тому, що модифікований метод надає змогу знаходити контури плями в явному вигляді.

Ключові слова: мультимедійний тир, лазерна пляма, контур, центр ваги, фільтри цифрового зображення.

Determining the centroid of a laser spot in the plane of a multimedia shooting gallery sensor based on the methods of interpolation and filtering of the image fragment / S. Yaremenko, Iu. Krak // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 3–11.

Abstract. The authors consider the problem of determining the position of the centroid of a laser spot on the plane of the photosensor in a multimedia shooting gallery. A two-stage approach to solving this problem is proposed. The possibilities of increasing the accuracy of determining the centroid by explicitly highlighting the contours of the spot (2nd stage of processing) instead of determining the boundaries of the laser spot through threshold binarization are investigated. The approaches to determining the contours of the spot are analyzed. To solve the problem, the scale of the image fragment was increased through the interpolation of new points. The possibilities of highlighting the contour of the spot by processing a fragment of the image with filters of low and high frequencies are investigated. A comparative assessment of the accuracy of the basic algorithm and that of the modified version was carried out, which showed that the modified algorithm increases the accuracy of determining the centroid by 30%. Higher accuracy was achieved because the modified method made it possible to find the explicit contours of the spot.

Keywords: multimedia shooting range, laser spot, contour, centroid, digital image filters.

==========

УДК 004.891.2:614.446

Інтелектуальна система підтримки прийняття рішень для епідеміологічної діагностики. ІІ. Інформаційні технології / К.О. Базілевич, Д.І. Чумаченко, Л.Ф. Гуляницький, Є.С. Меняйлов, С.В. Яковлев // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 12–23.

Анотація. У статті запропоновано компоненти інтелектуальної системи підтримки прийняття рішень для епідеміологічної діагностики та досліджено їхню взаємодію з користувачем. До складових системи включено банк моделей та методів машинного навчання, банк моделей популяційної динаміки, засоби візуалізації і формування звітів, блок формування управлінських рішень. Надано загальну концепцію інформаційної технології для гарантування біобезпеки населення. Розроблено модель варіантів використання зазначеної інформаційної технології користувачем та побудовано діаграму послідовностей. Запропоновано модель компонентів інформаційної технології та шляхи їх розгортання на сервері.

Ключові слова: система підтримки прийняття рішень, інформаційна технологія, епідеміологічна діагностика, машинне навчання, популяційна динаміка.

Intelligent decision support system for epidemiological diagnostics. II. Information technology development / K.O. Bazilevych, D.I. Chumachenko, L.F. Hulianytskyi, I.S. Meniailov, S.V. Yakovlev // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 12–23.

Abstract. The article projects the components of the intelligent decision support system for epidemiological diagnostics and investigates their interaction with the user. The system includes a bank of models and machine learning methods, a bank of population dynamics models, visualization and reporting tools, and management decision-making unit. The concept of information technology to ensure biosafety of the population is provided. A model of specified information technology use cases is developed and a sequence diagram is constructed. A model of information technology components and ways of their deployment on a server are proposed.

Keywords: decision support system, information technology, epidemiological diagnostics, machine learning, population dynamics.

==========

УДК 519.854.3
Алгоритм розв'язування супермодулярних (max, +) задач розмітки із самоконтролем на основі субградієнтного спуску / В.М. Кригін, Р.О. Хоменко // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 24–31.

Анотація. Розглянуто алгоритм, який для будь-якої поданої на вхід (max, +) задачі розмітки з цілочисельними вагами надасть на вихід одну з двох відповідей: або розв'язок у формі оптимальної розмітки, або фразу «задача не є супермодулярною», при цьому будь-яка відповідь гарантовано буде коректною. Самоконтроль у розпізнаванні образів полягає у тому, що не користувач приймає рішення, на яке питання треба відповісти, а сам алгоритм вирішує, що потрапляє у зону його компетентності. Іншою особливістю алгоритму є те, що він не потребує відомої впорядкованості міток для супермодулярних задач. Гарантію скінченної кількості кроків забезпечує використання субградієнтного спуску і цілочисельність ваг вершин та ребер.

Ключові слова: (max, +) задачі розмітки, супермодулярні задачі розмітки, самоконтроль у розпізнаванні образів, дискретна оптимізація, графові моделі, структурне розпізнавання образів.

Self-driven algorithm for solving supermodular (max, +) labeling problems based on subgradient descent / V. Krygin, R. Khomenko // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 24–31.

Abstract. An algorithm presented in this article gives a correct answer to one of the two questions for any (max, +) labeling problem with integer weights: either "What is the best labeling?" or "Is the problem supermodular?", and this answer is guaranteed to be correct. The algorithm is called self-driven because the user cannot decide which of the two questions will be answered — this decision is up to the algorithm. Also, the algorithm does not need to know the order of labels if the problem is supermodular. The finite execution time of the algorithm is guaranteed for integer weights of vertices and edges and use of subgradient descent.

Keywords: (max, +) labeling problems, supermodular labeling problems, self-driven pattern recognition, discrete optimization, graphical models, structural pattern recognition.

==========

СИСТЕМНИЙ АНАЛІЗ **SYSTEMS ANALYSIS**

УДК 519.217.2+616.006
Аналіз білкових структур плазми крові при гліомах з використанням Баєсових процедур розпізнавання на моделях ланцюгів Маркова / А.М. Гупал, А.Л. Тарасов // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 32–37.

Анотація. Розглянуто застосування Баєсових процедур розпізнавання на моделі ланцюгів Маркова до вивчення запальних процесів при гліомах. Проаналізовано показники білкових структур плазми крові при гліомах, метастазах та черепно-мозковому струсі, отримані за допомогою лазерного спектрографа. Зроблено порівняльний аналіз результатів розпізнавання на базі білкових структур за показниками поверхневого плазмового резонансу та модифікованої швидкості осідання еритроцитів при гліомах.

Ключові слова: Баєсові процедури розпізнавання, ланцюги Маркова, гліоми головного мозку, метастази, лазерний спектрограф, білкові структури плазми крові.

Analysis of protein structures of blood plasma in gliomas using Bayesian recognition procedures on the Markov chain model / A.M. Gupal, A.L. Tarasov // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 32–37.

Abstract. The authors consider the application of Bayesian recognition procedures on Markov chain models to the inflammatory processes in gliomas. Indicators of protein structures of blood plasma in gliomas, metastases, and craniocerebral disease obtained with the help of a laser spectrograph are analyzed. A comparative analysis of the results of recognition on the basis of protein structures in relation to the indicators of surface plasmon resonance and modified erythrocyte sedimentation rate in gliomas is carried out.

Keywords: Bayesian recognition procedure, Markov chains, brain gliomas, metastases, laser spectrograph, protein structures of blood plasma.

==========

УДК 519.21
Деякі багатовимірні стохастичні моделі керування запасами із сепарабельною функцією витрат / П.С. Кнопов, Т.В. Пепеляєва // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 38–45.

Анотація. Досліджено багатономеклатурні моделі теорії запасів з використанням фактів теорії багатокомпонентних керованих випадкових процесів. Розглянуто марковські та напівмарковські керовані стохастичні системи. Визначено структуру оптимальної стратегії для багатономенклатурної системи запасів.

Ключові слова: марковські процеси, керування запасами, (s, S)-стратегія, критерій оптимальності, оптимальна стратегія.

Some multi-dimentional stochastic models in inventory control with separable cost function / P.S. Knopov, T.V. Pepelyaeva // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 38–45.

Abstract. Multi-task models of the inventory theory are investigated with the use of the facts of the theory of multi-component controlled random processes. Markov and semi-Markov controlled stochastic systems are considered. The structure of optimal strategy for multi-task inventory system is determined.

Keywords: Markov processes, inventory control, (s, S)-strategy, optimality criterion, optimal strategy.

==========

УДК 519.85

Оптимізаційні задачі для максимального k-плекса / П.І. Стецюк, О.М. Хом'як, Є.А. Блохін, А.А. Супрун // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 46–58.

Анотація. Побудовано квадратичну оптимізаційну задачу для знаходження максимального k-плекса у неорієнтованому графі. Наведено два сімейства функціонально надлишкових квадратичних обмежень, які отримано за допомогою обмежень Булевої задачі для максимального k-плекса. Досліджено вплив функціонально надлишкових обмежень на покращення точності Лагранжевих двоїстих оцінок для цільової функції квадратичної задачі. Розроблено алгоритм пошуку всіх максимальних k-плексів та наведено результати тестових експериментів для його реалізації за допомогою програмного пакета GLPK (GNU Linear Programming Kit).

Ключові слова: максимальний k-плекс, максимальна кліка, квадратична оптимізаційна задача, Булева задача лінійного програмування, функціонально-надлишкове обмеження, Лагранжева двоїста оцінка.

Optimization problems for the maximum k-plex / P.I. Stetsyuk, O.M. Khomiak, Ye.A. Blokhin, A.A. Suprun // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 46–58.

Abstract. A quadratic optimization problem for finding the maximum k-plex in an undirected graph is constructed. Two families of superfluous quadratic constraints are presented, which are obtained by means of constraints of the Boolean linear programming problem for the maximum k-plex. The influence of superfluous constraints on the improvement of the accuracy of Lagrangian dual bounds for the objective function of the quadratic problem is investigated. An algorithm for searching all the maximum k-plexes is developed and the results of test experiments for its implementation using the GLPK software package (GNU Linear Programming Kit) are presented.

Keywords: k-plex, undirected graph, quadratic optimization problem, dual bound.

==========

УДК 519.85

Решітчасте покриття кубоїда мінімальною кількістю півсфер / Ю.Г. Стоян, Т.Є. Романова, О.В. Панкратов, А.Д. Тевяшев // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 59–69.

Анотація. Розглянуто задачу часткового решітчастого покриття кубоїда заданих розмірів мінімальною кількістю однакових півсфер із заданим коефіцієнтом покриття. Побудовано математичну модель у вигляді задачі змішаного цілочислового нелінійного програмування. Запропоновано метод розв'язання, в якому застосовано ідею релаксації задачі тривимірного покриття до задачі покриття прямокутної області сім'єю однакових кругів радіуса, що залежить від висоти кубоїда, радіуса півсфер та відстані між центрами сусідніх півсфер. Наведено результати обчислювальних експериментів для прикладної задачі оптимізації розміщення сенсорів у заданій тривимірній області.

Ключові слова: півсфера, решітчасте покриття, кубоїд, математична модель, оптимізація.

Lattice coverage of a cuboid with minimum number of semispheres / Yu. Stoyan, T. Romanova, O. Pankratov, A. Tevyashev // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 59–69.

Abstract. The problem of partial lattice coverage of a cuboid of given dimensions with a minimum number of identical hemispheres with a given coverage factor is considered. A mathematical model in the form of a mixed integer nonlinear programming problem is constructed. A solution algorithm is proposed. The problem of three-dimensional coverage is reduced to the problem of covering a rectangular area by a family of identical circles of radius that depends on the height of the cuboid, the radius of the hemispheres, and the distance between the centers of neighboring hemispheres. The results of computational experiments for the problem of optimizing the placement of sensors in a given three-dimensional domain are provided.

Keywords: hemisphere, lattice coverage, cuboid, mathematical model, optimization.

==========

УДК 517.9: 519.6

Деякі двовимірні крайові задачі фільтраційної динаміки для моделей з пропорційною похідною Капуто / В.М. Булавацький // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 70–81.

Анотація. Одержано замкнені розв'язки деяких двовимірних нестаціонарних крайових задач фільтраційної динаміки в тріщинувато-пористих пластах, поставлених для дробово-диференційних математичних моделей. Вказані математичні моделі побудовано з використанням узагальненої (пропорційної) похідної Капуто за часовою змінною та похідних Рімана–Ліувілля за геометричними змінними. Разом з прямою задачею розглянуто і двовимірну обернену крайову задачу визначення невідомої функції джерела, залежної лише від геометричних змінних. Наведено умови існування регулярних розв'язків розглянутих задач. Для окремого випадку лише часової нелокальності фільтраційного процесу розв'язана крайова залача з нелокальними граничними умовами.

Ключові слова: математичне моделювання, дробово-диференційна динаміка фільтраційних процесів, тріщинувато-пористі середовища, некласичні моделі, пропорційна похідна Капуто, похідна Рімана–Ліувілля, двовимірні крайові задачі, обернені задачі, задачі з нелокальними умовами, замкнені розв'язки.

Some two-dimensional boundary-value problems of filtration dynamics for models with proportional Caputo derivative / V.M. Bulavatsky // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 70–81.

Abstract. Closed solutions are obtained for some two-dimensional non-stationary boundary-value problems of filtration dynamics in fractured-porous formations, posed within the framework of fractional-differential mathematical models. These mathematical models are constructed using the generalized (proportional) Caputo derivative with respect to the time variable and Riemann–Liouville derivatives with respect to geometric variables. Along with the direct problem, we also consider a two-dimensional inverse boundary-value problem for determining the unknown source function that only depends on geometric variables. Conditions for the existence of regular solutions of the considered problems are given. For a separate case of only time nonlocality of the filtration process, a boundary-value problem with nonlocal boundary conditions is solved.

Keywords: mathematical modeling, fractional-differential dynamics of filtration processes, fractured-porous media, non-classical models, proportional Caputo derivative, Riemann–Liouville derivative, two-dimensional boundary-value problems, inverse problems, problems with non-local conditions, closed-form solutions.

==========

УДК 517.988

Збіжність методу екстраполяції з минулого для варіаційних нерівностей в рівномірно опуклих Банахових просторах / В.В. Семенов, С.В. Денисов // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 82–93.

Анотація. Досліджено два нові алгоритми для розв'язання варіаційних нерівностей у Банахових просторах. Перший алгоритм — модифікація двоетапного методу Попова, що використовує узагальнену проєкцію Альбера замість метричної. Другий алгоритм є адаптивним варіантом першого, де використовується правило поновлення величини кроку, що не вимагає знання Ліпшицевих констант та обчислень значень оператора в додаткових точках. Для варіаційних нерівностей з монотонними, Ліпшицевими операторами, що діють в 2-рівномірно опуклому та рівномірно гладкому Банаховому просторі, доведено теореми про слабку збіжність методів.

Ключові слова: варіаційна нерівність, монотонний оператор, узагальнена проєкція Альбера, 2-рівномірно опуклий Банахів простір, рівномірно гладкий Банахів простір, алгоритм, збіжність.

Convergence of extrapolation from the past method for variational inequalities in uniformly convex Banach spaces / V.V. Semenov, S.V. Denisov // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 82–93.

Abstract. The authors analyze two new algorithms for solving variational inequalities in Banach spaces. The first algorithm is a modification of Popov's two-stage method that uses the Albert generalized projection instead of the metric one. The second algorithm is an adaptive version of the first one, where the step size update rule is used, which does not require knowledge of the Lipschitz constants and calculation of the operator values at additional points. For variational inequalities with monotone, Lipschitz operators acting in a 2-uniformly convex and uniformly smooth Banach space, theorems on the weak convergence of the methods are proved.

Keywords: variational inequality, monotone operator, Albert generalized projection, 2-uniformly convex Banach space, uniformly smooth Banach space, algorithm, convergence.

==========

УДК 519.6

Узагальнення моделі противірусної імунної відповіді для комплексного урахування дифузійних збурень, температурної реакції організму та логістичної популяційної динаміки антигенів / С.В. Барановський, А.Я. Бомба, С.І. Ляшко // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 94–111.

Анотація. Узагальнено математичну модель Марчука–Петрова противірусної імунної відповіді для комплексного урахування дифузійних збурень, зосереджених впливів, температурної реакції організму та логістичної популяційної динаміки вірусних елементів і антитіл на розвиток інфекційного захворювання. Розроблено покрокову процедуру чисельно-асимптотичного розв'язання відповідних сингулярно збурених задач із запізненнями. Наведено результати комп'ютерного моделювання, які ілюструють вплив «модельного» зниження максимального рівня кількості антигенів в епіцентрі зараження внаслідок їхнього дифузійного «розсіювання», температурної реакції організму та логістичної популяційної динаміки вірусів на характер перебігу інфекційного захворювання, зокрема і за наявності зосереджених джерел антигенів. Зазначено, що така системна дія вказаних чинників може спричинити зниження початково надкритичної концентрації антигенів до рівня, після якого їхню нейтралізацію і виведення з організму буде забезпечено наявним рівнем імунного захисту, що є важливим під час прийняття рішень щодо необхідності застосування зовнішнього «лікувального» впливу.

Ключові слова: модель противірусної імунної відповіді, динамічні системи із запізненням, асимптотичні методи, сингулярно збурені задачі, зосереджені впливи, логістична динаміка.

Generalization of the antiviral immune response model for complex consideration of diffusion perturbations, body temperature response, and logistic antigens population dynamics / S.V. Baranovsky, A.Ya. Bomba, S.I. Lyashko // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 94–111.

Abstract. The Marchuk–Petrov mathematical model of antiviral immune response is generalized for complex consideration of diffusion perturbations, concentrated influences, body temperature response, and logistic population dynamics of viral elements and antibodies to the development of infectious disease. A step-by-step procedure for numerically asymptotic solution of the corresponding singularly perturbed problems with delays is developed. The authors present the results of computer simulation, which illustrate the "model" reduction of the maximum level of antigens in the epicenter of infection due to their diffusion "scattering," body temperature response, and logistic population dynamics of viruses on the nature of infectious disease, including the presence of concentrated sources of antigens. It is emphasized that such a systemic effect of these factors can reduce the initial supercritical concentration of antigens to a level after which their neutralization and excretion will be provided by the existing level of immune protection, which is important in deciding whether to use external "therapeutic" effects.

Keywords: model of antiviral immune response, dynamic systems with delay, asymptotic methods, singularly perturbed problems, concentrated influences, logistic dynamics.

==========

УДК 519.22

Метод оптимізації надійності, альтернативний bPOE / В.А. Пепеляєв, О.М. Голодніков, Н.О. Голоднікова // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 112–116.

Анотація. Розроблено новий метод оптимізації надійності, альтернативний методу bPOE. Для порівняння ефективності роботи запропонованого методу та оригінального методу bPOE було проведено чисельні експерименти з використанням двох різних наборів даних. Аналіз результатів обчислень показав, що вони однакові для обох методів.

Ключові слова: bPOE, CVaR, мінімізація ймовірності відмов, хвіст функції розподілу, функція втрат, поріг.

Reliability optimization method alternative to bPOE / V.A. Pepelyaev, A.N. Golodnikov, N.A. Golodnikova // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 112–116.

Abstract. A new method of reliability optimization, alternative to the bPOE method, is developed. To compare the efficiency of the proposed method and of the original bPOE method, numerical experiments were performed using two different data sets. Analysis of the calculations showed that both methods gave the same results.

Keywords: bPOE, CVaR, minimization of failure probability, tail distribution function, loss function, threshold.

==========

УДК 519.6

Математичне моделювання стану динамічних мультиплікативно нелінійних систем / В.А. Стоян // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 117–128.

Анотація. Поставлено і за середньоквадратичним критерієм розв'язано початково-крайові задачі динаміки нелінійних просторово розподілених систем. Розглянуто системи, математична модель яких побудована добутком двох (або кількох) диференціальних перетворень їхніх функції стану. Будуються аналітичні залежності цієї функції за наявності дискретно і неперервно визначених початково-крайових спостережень за ними, без обмежень на кількість та якість останніх. Оцінено точність множин отриманих розв'язків та досліджено їхню однозначність.

Ключові слова: нелінійні динамічні системи, системи з невизначеностями, системи з розподіленими параметрами, просторово розподілені системи, псевдорозв'язки, некоректні початково-крайові задачі.

Mathematical modeling of the state of dynamic multiplicative nonlinear systems / V.A. Stoyan // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 117–128.

Abstract. The author formulates and solves, by the root-mean-square criterion, the initial-boundary-problems of the dynamics of nonlinear spatially distributed systems. Systems whose mathematical model is generated by the product of two or more differential transformations of their functions of state are considered. Analytical dependencies of this function are constructed in the presence of their discretely and continuously defined initial-boundary observations, without constraints for the number and quality of the latter. The accuracy of the sets of the obtained solutions is evaluated and their uniqueness is analyzed.

Keywords: nonlinear dynamical systems, systems with uncertainties, systems with distributed parameters, spatially distributed systems, pseudosolutions, ill-posed initial-boundary-value problems.

==========

УДК 004.056.55

Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 129–138.

Анотація. Розроблено теоретичні основи асиметричного шифрування на базі системи залишкових класів та її модифікованої досконалої форми. При цьому модулі системи залишкових класів являють собою таємні ключі. Під час відновлення числа за його залишками множення відбувається на довільно вибрані коефіцієнти (відкриті ключі). Встановлено, що криптостійкість запропонованих алгоритмів ґрунтується на розв'язанні задачі факторизації або повного перебору наборів модулів. Розроблені підходи дають змогу практично необмежено збільшувати блок відкритого тексту, усуваючи необхідність використання різних режимів шифрування.

Ключові слова: система залишкових класів, криптоалгоритм, асиметрична криптосистема, шифртекст, криптоаналіз, стійкість.

Residue number system asymmetric cryptoalgorithms / Ya.M. Nykolaychuk, I.Z. Yakymenko, N.Ya. Vozna, M.M. Kasianchuk // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 129–138.

Abstract. Theoretical foundations of asymmetric encryption based on the residue number system and its modified perfect form are developed. The selected moduli of the residue number system are considered to be secret keys. When recovering a number from its residues, multiplication by arbitrarily selected coefficients (public keys) takes place. It is established that cryptostability of the proposed algorithms is based on solving the problem of factorization or exhaustive search of sets of moduli. The developed approaches allow us to increase the block of plaintext almost indefinitely, eliminating the need to use different encryption modes.

Keywords: residue number system, cryptoalgorithm, asymmetric cryptosystem, ciphertext, cryptanalysis, stability.

==========

УДК 519.6

Оптимізація багаторозрядної операції множення на основі дискретних перетворень (Фур'є, косинусних, синусних) у паралельній моделі обчислення / В.К. Задірака, А.М. Терещенко // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 139–161.

Анотація. Розглянуто операцію багаторозрядного множення, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів. Запропоновано алгоритми реалізації операції множення двох -розрядних чисел на основі дискретних косинусних та синусних перетворень (ДКП та ДСП). За рахунок використання ДКП та ДСП розділено обчислення для дійсної та уявної частин дискретного перетворення Фур'є (ДПФ) дійсного сигналу парної довжини, що дає змогу перевести обчислення з поля комплексних чисел у поле дійсних чисел та зменшити складність багаторозрядної операції множення за кількістю однорозрядних операцій комплексного множення. Проведено заміну операцій алгоритму для збереження симетрії у дійсній або уявній частинах багаторозрядних чисел, що дає змогу використовувати ДКП та ДСП меншої розрядності $N / 2 + 1$ та розширює можливості з розпаралелювання під час реалізації багаторозрядного множення.

Ключові слова: багаторозрядне множення, багаторозрядна арифметика, асиметрична криптографія, дискретне косинусне перетворення, дискретне синусне перетворення, дискретне перетворення Фур'є, швидкий алгоритм обчислення Фур'є.

Optimization of multidigit multiplication based on discrete transforms (Furie, cosine, sine) in parallel computational model / V.K. Zadiraka, A.M. Tereshchenko // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 139–161.

Abstract. This paper considers the multidigit multiplication operation, on whose speed the speed of asymmetric cryptographic software and hardware depends. Algorithms for implementation of the multiplication of two-digit numbers based on discrete cosine and sine transforms (DCT and DST) are proposed. Due to the use of DCT and DST, the calculations for the real and imaginary parts of the discrete Fourier transform (DFT) of a real even-length signal are separated, which allows translating the complex number calculations to real number calculations. Algorithm operations are replaced to preserve symmetry in real or imaginary parts of multidigit numbers, which allows the use of DCT and DST of lower length $N / 2 + 1$ and increases the possibility of parallelism in the implementation of multidigit multiplication.

Keywords: multidigit multiplication, multidigit arithmetic, asymmetric cryptography, discrete cosine transform, discrete sine transform, discrete Fourier transform, fast Fourier calculation algorithm.

==========

УДК 004
Технології віртуалізації, що властиві живим істотам / О.В. Палагін, М.В. Семотюк // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 162–171.

Анотація. Розглянуто одну із складових інформаційних технологій — технології віртуалізації, що властиві винятково живим істотам. Показано взаємозв'язок технологій віртуалізації з іншими складовими інформаційних технологій, як-от кількісні технології, технології даних, технології знань. На прикладі моделі внутрішнього вуха людини продемонстровано, як технології віртуалізації працюють на практиці, даючи змогу одні фізичні параметри замінювати на інші в тому разі, коли можливості живої істоти є обмеженими.

Ключові слова: інформаційні технології, рівні технологій, технології віртуалізації, технології даних, технології знань, верифікація, стоячі хвилі, біжуча хвиля, поперечний резонанс, уявний експеримент, фізичний експеримент, віртуальне слідування, внутрішнє вухо, завитка, мембрана Рейснера, базилярна мембрана, квантування.

Technologies of virtualizatin of living beings / O.V. Palagin, M.V. Semotiuk // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 162–171.

Abstract. The authors consider one of the components of information technology — virtualization technologies, which are unique to living beings. The relationship of virtualization technologies with other components of information technologies, such as quantitative technologies, data technologies, knowledge technologies, is shown. Using the model of the human inner ear as an example, it is shown how they work in practice, allowing some physical parameters to be replaced by others when the possibilities of a living being are limited.

Keywords: information technologies, technology levels, virtualization technologies, data technologies, knowledge technologies, verification, standing waves, traveling wave, transverse resonance, imaginary experiment, physical experiment, virtual following, inner ear, helix, Reissner's membrane, basilar membrane, quantization.

==========

УДК 516.813
Алгебраїчні операції над нечіткими множинами і відношеннями в автоматній інтерпретації з реалізацією логіковими апаратними засобами / С.Л. Кривий, В.М. Опанасенко, С.Б. Зав'ялов // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 172–182.

Анотація. Розглянуто алгебраїчні операції над нечіткими множинами і відношеннями та їхня реалізація апаратними засобами в автоматній інтерпретації. Описано два способи зображення значень функцій належності нечітких множин та методи перетворення таких зображень. Наведено відповідні оцінки складності виконання операцій з такими зображеннями та обгрунтування коректності алгоритмів.

Ключові слова: нечіткі множини, відношення, алгебраїчні операції, скінченні автомати, FPGA.

Algebraic operations over fuzzy sets and relations in automata interpretation with realization by logical hardware means / S.L. Kryvyi, V.M. Opanasenko, S.B. Zavyalov // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 172–182.

Abstract. Algebraic operations over fuzzy sets and relations and their implementation by hardware in automata interpretation are considered. Two ways of representing the values of membership functions of fuzzy sets and methods of transformation of such images are described. Appropriate estimates of the complexity of operations with such images are given and correctness of the algorithms is substantiated.

Keywords: fuzzy sets, fuzzy relations, algebraic operations, finite automata, FPGA.

==========

УДК 519.64 + 519.86: 53.072
Канонічні рівняння оптичного гістерезису / В.М. Старков // Кібернетика та системний аналіз. 2022. Том 58, № 4. С. 183–194.

Анотація. Роботу виконано у контексті конкурентної ідеології створення елементної бази цифрових оптичних комп'ютерів (трансфазори, оптичні ключі, осередки пам'яті) на відмінній від інтерферометра Фабрі–Перо основі. Докладно розглянуто математичні моделі стаціонарної (варіант I) та нестаціонарної (варіант II) чотирипучкової лазерної взаємодії в оптично-нелінійних середовищах у вигляді системи звичайних диференційних рівнянь із заданими граничними умовами (I) та системи інтегро-диференційних рівнянь із граничними умовами (II). Введено оригінальні шукані функції $z(x)$ (I) та $u(z,t)$, $v(z,t)$ (II). Завдяки цьому розв'язання задачі (I) зведено до розв'язання простого трансцендентного рівняння (канонічного рівняння оптичного гістерезису), а розв'язання задачі (II) — до розв'язання системи двох нелінійних інтегральних рівнянь відносно амплітуд інтерференційних картин (канонічної системи рівнянь нестаціонарного оптичного гістерезису).

Ключові слова: бістабільність, гістерезис, оптичний комп'ютер, математична модель, лазерна взаємодія, інтегральне рівняння.

Canonical equation of optical hysteresis / V. Starkov // Kibernetyka ta Systemnyi Analiz. 2022. Vol. 58, N 4. P. 183–194.

Abstract. The content of the study is in line with the competitive ideology of creating the element base of digital optical computers (transphasors, optical switches, memory devices) on a basis other than the Fabry–Perot interferometer. Mathematical models of stationary (variant I) and nonstationary (variant II) four-beam laser interaction in optically nonlinear media are considered in detail in the form of a system of ordinary differential equations with given boundary conditions (I) and a system of integro-differential equations with boundary conditions (II). The original desired functions $z(x)$ (I) and $u(z,t)$, $v(z,t)$ (II) are introduced. As a result, the solution of problem (I) is reduced to solving a simple transcendental equation (canonical equation of optical hysteresis), and the solution of problem (II) is reduced to a system of two nonlinear integral equations with respect to the amplitudes of interference patterns (canonical system of equations of nonstationary optical hysteresis).

Keywords: bistability, hysteresis, optical computer, mathematical model, laser interaction, integral equation.