КІБЕРНЕТИКА **CYBERNETICS**

УДК 004.274

Совместное использование методов структурной декомпозиции для оптимизации схемы микропрограммного автомата Мура / А.А. Баркалов, Л.А. Титаренко, А.В. Баев, А.В. Матвиенко // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 3–16.

Аннотация. Предложен метод оптимизации аппаратурных затрат в схеме автомата Мура, реализуемой в базисе FPGA. Метод основан на одновременном использовании замены входов и преобразования кодов состояний в коды классов псевдоэквивалентных состояний. Такой подход приводит к трехуровневой схеме автомата. Приведен пример синтеза автомата Мура с использованием предложенного метода и выполнен анализ его положительных и отрицательных характеристик. Исследования на базе стандартных автоматов показали, что данный метод позволяет уменьшить аппаратурные затраты и потребляемую мощность при незначительной потере быстродействия.

Ключевые слова: автомат Мура, синтез, FPGA, LUT, структурная декомпозиция.

Спільне використання методів структурної декомпозиції для оптимізації схеми мікропрограмного автомата Мура / О.О. Баркалов, Л.О. Тітаренко, А.В. Баєв, О.В. Матвієнко // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 3–16.

Анотація. Запропоновано метод оптимізації апаратурних витрат в схемі автомата Мура, що реалізується в базисі FPGA. Метод ґрунтується на одночасному використанні заміни входів і перетворення кодів станів у коди класів псевдоеквівалентних станів. Такий підхід призводить до трирівневої схеми автомата. Наведено приклад синтезу автомата Мура з використанням запропонованого методу і виконано аналіз позитивних і негативних його характеристик. Дослідження на базі стандартних автоматів показали, що запропонований метод дає змогу зменшити апаратурні витрати і споживану потужність із незначною втратою швидкодії.

Ключові слова: автомат Мура, синтез, FPGA, LUT, структурна декомпозиція.

Joint using methods of structural decomposition for optimizing circuit of Moore FSM / A.A. Barkalov, L.A. Titarenko, A.V. Baiev, A.V. Matviienko // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 3–16.

Abstract. A method is proposed for optimizing hardware amount in the circuit of Moore FSM implemented with FPGA. The method is based on joint using replacement of inputs and transformation of state codes into codes of classes of pseudoequivalent states. This approach leads to a three-level circuit of FSM. There is shown an example of synthesis of Moore FSM with application of the proposed method. Analysis of positive and negative features of the proposed method is conducted. The researches on the base of standard benchmark FSM show that the proposed method allows reducing hardware amount and consumed power with insignificant degradation of FSM performance.

Keywords: Moore FSM, synthesis, FPGA, LUT, structural decomposition.

==========

УДК 519-7/339.9

Оптимизация выбора элементов математического обеспечения в системах управления с существенно разноскоростными процессами / В.В. Хиленко, А.В. Степанов, И. Котуляк, М. Райис // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 17–22.

Аннотация. Проведен сравнительный анализ различных методов решения задачи определения спектральных характеристик математических моделей систем управления (систем поддержки принятия решений). Рекомендован выбор метода с учетом специфики объекта или технологического процесса. На основании проведенных модельных экспериментов сделан вывод о преимуществах использования степенного метода и метода Хиленко, когда диапазон изменения скоростей рассчитываемых переменных неизвестен или может существенно измениться при изменении режимов работы объекта (технологического процесса), а также при возникновении критических ситуаций и необходимости их «отработки» системой управления.

Ключевые слова: системы управления, системы поддержки принятия решений, математическое и программно-алгоритмическое обеспечение, определение спектральных характеристик, метод Леверье–Ньютона, метод Хиленко, степенной метод.

Оптимізація вибору елементів математичного забезпечення в системах керування з істотно різношвидкісними процесами / В.В. Хиленко, О.В. Степанов, І. Котуляк, М. Раїс // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 17–22.

Анотація. Проведено порівняльний аналіз різних методів розв’язання задачі визначення спектральних характеристик математичних моделей систем керування (систем підтримки прийняття рішень). Запропоновано вибір методу з урахуванням специфіки об’єкта або технологічного процесу. На підставі проведених модельних експериментів зроблено висновок про переваги використання степеневого методу і методу Хиленка, коли діапазон зміни швидкостей змінних, що розраховуються, невідомий або може істотно змінитися із зміною режимів роботи об’єкта (технологічного процесу), а також у разі виникнення критичних ситуацій і необхідності їхнього «відпрацювання» системою керування.

Ключові слова: системи керування, системи підтримки прийняття рішень, математичне та програмно-алгоритмічне забезпечення, визначення спектральних характеристик, метод Левер'є–Ньютона, метод Хиленка, степеневий метод.

Optimization of the selection of software elements in control systems with significantly different-speed processes / V.V. Khilenko, O.V. Stepanov, I. Kotuliak, M. Reis // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 17–22.

Abstract. A comparative analysis of various methods for solving the problem of determining the spectral characteristics of mathematical models of control systems is carried out, if the dynamics of the object contains processes that differ significantly in speed. Based on the model experiments carried out, a conclusion was made about the advantages of using the power-law method and the Khilenko method, when the range of variation of the rates of the calculated variables is unknown or can change significantly when changing the operating modes of the object (technological process), as well as in the event of critical situations and the need to "work out" them by control system.

Keywords: control systems, decision support systems, mathematical and software-algorithmic support, determination of spectral characteristics, Le Verrier–Newton method, Khilenko method, power method.

==========

УДК 519.7

Достижимая верхняя граница sup-нормы произведения элементов кольца усеченных многочленов и ее применение к анализу NTRU-подобных криптосистем / А.Н. Алексейчук, А.А. Матийко // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 23–29.

Аннотация. Получен ответ на вопрос, поставленный в 2008 г. В. Любашевским, об эффективном алгоритме вычисления параметра $\theta(f)$, характеризующего величину sup-нормы произведения элементов кольца усеченных многочленов по модулю заданного унитарного многочлена $f(x)$ с вещественными коэффициентами. Рассмотрено применение полученных результатов к оцениванию вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах.

Ключевые слова: решеточная криптография, кольцо усеченных многочленов, sup-норма произведения многочленов, NTRU-подобная криптосистема, вероятность ошибочного расшифрования.

Досяжна верхня межа sup-норми добутку елементів кільця зрізаних поліномів та її застосування до аналізу NTRU-подібних криптосистем / А.М. Олексійчук, О.А. Матійко // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 23–29.

Анотація. Отримано відповідь на питання, поставлене в 2008 р. В. Любашевським, про ефективний алгоритм обчислення параметра $\theta(f)$, що характеризує величину sup-норми добутку елементів кільця зрізаних поліномів за модулем заданого унітарного полінома $f(x)$ з дійсними коефіцієнтами. Розглянуто застосування отриманих результатів до оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних криптосистемах.

Ключові слова: решіткова криптографія, кільце зрізаних поліномів, sup-норма добутку поліномів, NTRU-подібна криптосистема, ймовірність помилкового розшифрування.

Achievable upper bound for the sup-norm of the elements' product in the ring of truncated polynomials and its application to the analysis of NTRU-like cryptosystems / **A.N. Alekseychuk, A.A. Matiyko** // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 23–29.

Abstract. The answer to the question posed in 2008 by V. Lyubashevsky about an efficient algorithm for calculating the parameter $\theta(f)$ that characterizes the value of the sup-norm of the elements' product in the ring of truncated polynomials modulo a given mimic polynomial $f(x)$ with real coefficients is obtained. The application of the obtained results to the estimation of decryption failure probability of messages in NTRU-like cryptosystems is considered.

Keywords: lattice-based cryptography, truncated polynomial ring, sup-norm of polynomials' product, NTRU-like cryptosystem, decryption failure probability.

==========

Комбинаторные конфигурации в определении антимагических разметок графов / М.Ф. Семенюта // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 30–40.

Аннотация. Формализовано определение разметки графа в терминах комбинаторных конфигураций. Исследована связь реберных и вершинных (a, d)-дистанционных антимагических разметок с такими известными конфигурациями, как разделяющие системы и множества магических прямоугольников. Получено решение задачи построения этих разметок для отдельных типов графов и определенных значений a, d.

Ключевые слова: комбинаторная конфигурация, разделяющая система, множество магических прямоугольников, регулярный граф, бирегулярный граф, антимагическая разметка, (a, d)-дистанционная антимагическая разметка.

УДК 519.1
Комбінаторні конфігурації у визначенні антимагічних розміток графів / М.Ф. Семенюта // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 30–40.

Анотація. Формалізовано визначення розмітки графу в термінах комбінаторних конфігурацій. Досліджено зв'язок реберних та вершинних (a, d)-дистанційних антимагічних розміток з такими відомими конфігураціями, як відокремлювальні системи і множини магічних прямокутників. Отримано розв'язок задачі побудови цих розміток для окремих типів графів і певних значень a, d.

Ключові слова: комбінаторна конфігурація, відокремлювальна система, множина магічних прямокутників, регулярний граф, бірегулярний граф, антимагічна розмітка, -дистанційна антимагічна розмітка.

Combinatorial configurations in determination of antimagiclabelings of graphs / M.F. Semeniuta // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 30–40.

Abstract. We have formalized the definition of graph labeling in terms of combinatorial configurations. We have investigated the connection between edge and vertex (a, d)-distance antimagic labelings with such well-known configurations as separating systems and magic rectangle set. We have obtained a solution to the problem of construction of indicated labelings for some types of graphs and certain values a, d.

Keywords: combinatorial configuration, separating system, magic rectangle set, regular graph, bi-regular graph, antimagic labeling, (a, d)-distance antimagic labeling.

==========

УДК 681.322.012
Быстрый рекурсивный алгоритм умножения матриц порядка $n = 3^q (q > 1)$ / Л.Д. Елфимова // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 41–51.

Аннотация. Предложен новый быстрый рекурсивный алгоритм умножения матриц порядка $n = 3^q$ $(q > 1)$, построенный на основе гибридного алгоритма умножения матриц нечетного порядка $n = 3\mu$ $(\mu = 2q - 1, q > 1)$, который используется в качестве базового алгоритма при $\mu = 3^q$ $(q > 0)$. По сравнению с известным блочно-рекурсивным алгоритмом Лейдермана представленный алгоритм позволяет минимизировать на 10.4% мультипликативную сложность, равную $W_{\text{м}} \approx 0.896n^{2.854}$ операций умножения на глубине рекурсии $d = \log_3 n - 3$, и сократить вектор вычислений на три рекурсивных шага. Дана оценка мультипликативной сложности базового и рекурсивного алгоритмов.

Ключевые слова: линейная алгебра, блочно-рекурсивный алгоритм Лейдермана, семейство быстрых гибридных алгоритмов умножения матриц, алгоритм Винограда для скалярного произведения.

Швидкий рекурсивний алгоритм множення матриць порядку $n = 3^q$ $(q > 1)$ / Л.Д. Єлфімова // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 41–51.

Анотація. Запропоновано новий швидкий рекурсивний алгоритм множення матриць порядку $n = 3^q$ $(q > 1)$, побудований на основі гібридного алгоритму множення матриць непарного порядку $n = 3\mu$ $(\mu = 2q - 1, q > 1)$, який застосовується як базовий алгоритм, коли $\mu = 3^q$ $(q > 0)$. Порівняно з відомим блочно-рекурсивним алгоритмом Лейдермана наведений алгоритм дозволяє мінімізувати на 10.4% мультиплікативну складність, яка дорівнює $W_{\text{м}} = 0.896n^{2.854}$ операцій множення на глибині рекурсії $d = \log_3 n - 3$, та скоротити вектор обчислень на три рекурсивних кроки. Наведено оцінку мультипликативної складності базового та рекурсивного алгоритмів.

Ключові слова: лінійна алгебра, блочно-рекурсивний алгоритм Лейдермана, сім'я швидких гібридних алгоритмів множення матриць, алгоритм Винограда для скалярного добутку.

A fast recursive algorithm for multiplying matrices of order $n = 3^q$ $(q > 1)$ / L.D. Jelfimova // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 41–51.

Abstract. A new fast recursive algorithm is proposed for multiplying matrices of order $n = 3^q$ $(q > 1)$. This algorithm is based on hybrid algorithm for multiplying matrices of odd order $n = 3\mu$ $(\mu = 2q - 1, q > 1)$, which is used as basic algorithm for $\mu = 3^q$ $(q > 0)$. As compared with the well-known block-recursive Laderman's algorithm, the new algorithm minimizes by 10.4% the multiplicative complexity equal to $W_{\text{м}} = 0.896n^{2.854}$ multiplication operations at recursive level $d = \log_3 n - 3$ and reduces the computation vector by three recursive steps. The multiplicative complexity of the basic and recursive algorithms are estimated.

Keywords: linear algebra, Laderman's block-recursive matrix multiplication algorithm, family of fast hybrid matrix multiplication algorithms, Winograd's algorithm for inner product.

==========

УДК 519.6

Оптимизация погрешности в операторах интерлинации функции на *M* параллельных прямых / И.В. Сергиенко, О.Н. Литвин, О.О. Литвин, А.В. Ткаченко , А.А. Билобородов // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 52–61.

Аннотация. Рассмотрена задача оценки погрешности и оптимизации выбора параметров в операторах интерлинации эрмитового типа функций на системе *M* параллельных прямых. Для этого использованы формулы обобщенной эрмитовой интерлинации, которые в отличие от формул обычной эрмитовой интерлинации позволяют автоматически сохранять тот же класс дифференцируемости, к которому принадлежит приближенная функция. При построении этих операторов использована произвольная система не равных друг другу чисел $\beta_0, \beta_1, \ldots, \beta_N$. Предложен метод оптимального выбора этих параметров и оценка погрешности остатка.

Ключевые слова: интерлинация, оператор, остаток, оптимизация.

Оптимізація похибки в операторах інтерлінації функції на *M* паралельних прямих / І.В. Сергієнко, О.М. Литвин, О.О. Литвин, О.В. Ткаченко , А.А. Білобородов // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 52–61.

Анотація. Розглянуто питання оцінки похибки та оптимізації вибору параметрів в операторах інтерлінації функції ермітового типу на системі *M* паралельних прямих. Для цього застосовано формули узагальненої ермітової інтерлінації, які на відміну від формул звичайної ермітової інтерлінації надають змогу автоматично зберігати той самий клас диференційовності, якому належить наближувана функція. Під час побудови цих операторів використано довільну систему не рівних одне одному чисел $\beta_0, \beta_1, \ldots, \beta_N$. Запропоновано метод оптимального вибору цих параметрів та оцінку похибки залишку.

Ключові слова: інтерлінація, оператор, залишок, оптимізація.

Optimization of the error in the operators of interlineation of a function on *M* parallel lines / I.V. Sergienko, O.M. Lytvyn, O.O. Lytvyn, O.V. Tkachenko , A.A. Biloborodov // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 52–61.

Abstract. This article discusses the issue of estimating the error and optimizing the choice of parameters in Hermitian-type operators of interlineation of functions on a system of *M* parallel lines. For this, the formulas of generalized Hermitian-type interlineation are used, which, unlike the formulas of ordinary Hermitian-type interlineation, allow automatically preserving the same class of differentiability to which the approximate function belongs. When constructing these operators, an arbitrary system of unequal each other numbers $\beta_0, \beta_1, \ldots, \beta_N$ is used. The article proposes a method for the optimal choice of these parameters and an estimation of error of the remainder.

Keywords: interlineation, operator, remainder, optimization.

==========

УДК 519.217.2

Определение групп рисков при заболеваниях, сопутствующих COVID-19 / А.А. Вагис, А.М. Гупал, И.В. Сергиенко // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 62–68.

Аннотация. Для каждого заболевания существует определенный набор генов, мутации в которых увеличивают риск развития болезни. Массовое секвенирование ДНК больных и здоровых людей привело к определению генов, связанных с конкретными заболеваниями. Описаны эффективные процедуры определения мутаций и их месторасположения в последовательностях генов исследуемых пациентов. Предложено использовать оптимальную байесовскую процедуру определения групп рисков при конкретных заболеваниях, в том числе сопутствующих COVID-19.

Ключевые слова: секвенирование ДНК, точечные мутации, байесовская процедура распознавания.

Визначення груп ризиків для захворювань, супутних COVID-19 / О.А. Вагіс, А.М. Гупал, І.В. Сергієнко // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 62–68.

Анотація. Для кожного захворювання існує певний набір генів, мутації в яких збільшують ризик розвитку хвороби. Масове секвенування ДНК хворих і здорових людей допомогло визначити гени, пов'язані з конкретними захворюваннями. Описано ефективні процедури визначення мутацій та їхнього розташування в послідовності генів досліджуваних пацієнтів. Запропоновано використовувати оптимальну баєсівську процедуру визначення груп ризиків для конкретних захворювань, зокрема супутних COVID-19.

Ключові слова: секвенування ДНК, точкові мутації, баєсівська процедура розпізнавання.

Determination of groups of risks at the diseases COVID-19 / A.A. Vagis, A.M. Gupal, I.V. Sergienko // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 62–68.

Abstract. For every disease there is the concrete set of genes the mutations of which multiply the risk of development of illness. Determination of DNA of sick and healthy people resulted in determination of the genes, related to the concrete diseases. The effective procedures are described to determine the point mutations in sequences of the genes. On the basis of Bayesian procedure of recognition it is possible effectively to determine the groups of risks of diseases which COVID-19 accompanies.

Keywords: determination of DNA, the points mutations, Bayesian procedure of recognition.

==========

УДК 303.732+004.62+004.912+351/354

Лингвистический анализ данных интернет-медиа и социальных сетей в задачах оценивания общественных преобразований / М.З. Згуровский, Д.В. Ланде, А.А. Болдак, К.В. Ефремов, М.Н. Перестюк // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 69–80.

Аннотация. Разработан комбинированный подход к оценке эффективности общественных преобразований как меры несогласованности между действиями власти и ожиданиями общества и синергии (социальной активности) людей, основанный на формализованном согласовании результатов, полученных методом экспертных оценок и методами сентимент-анализа и интеллектуального анализа текстовых сообщений из открытых онлайн-источников и социальных сетей. Эти методы реализованы в виде комплекса веб-сервисов и приложений в среде разработки интегрированной он-лайн платформы Advanced Analytics Мирового центра данных «Геоинформатика и устойчивое развитие». Эффективность предложенного подхода продемон- стрирована на примере количественного оценивания отношения населения Украины к действиям власти, направленным на противодействие распространения эпидемии COVID-19.

Ключевые слова: вектор действий власти, вектор ожиданий общества, вектор преобразований (реформ), лингвистический анализ, контент-анализ, анализ данных Интернет медиа и социальных сетей, разведка на основе открытых источников.

Лінгвістичний аналіз даних інтернет-медіа та соціальних мереж у задачах оцінювання суспільних перетворень / М.З. Згуровський, Д.В. Ланде, А.О. Болдак, К.В. Єфремов, М.М. Перестюк // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 69–80.

Анотація. Розроблено комбінований підхід до оцінювання ефективності суспільних перетворень як міри неузгодженості між діями влади і очікуваннями суспільства та синергії (соціальної активності) людей, що ґрунтується на формалізованому узгодженні результатів, отриманих методом експертних оцінок, а також методами сентимент-аналізу та інтелектуального аналізу текстових повідомлень з відкритих онлайн-джерел і соціальних мереж. Ці методи реалізовано у вигляді комплексу вебсервісів та застосунків у середовищі розроблення інтегрованої онлайн-платформи Advanced Analytics Світового центру даних «Геоінформатика і сталий розвиток». Ефективність запропонованої методики продемонстровано на прикладі кількісного оцінювання ставлення населення України до дій влади, спрямованих на протидію поширенню епідемії COVID-19.

Ключові слова: вектор дій влади, вектор очікувань суспільства, вектор перетворень (реформ), лінгвістичний аналіз, контент-аналіз, аналіз даних інтернет-медіа та соціальних мереж, розвідка за відкритими джерелами.

Linguistic analysis of internet media and social networks datain problems on assessment of social transformations / M. Zgurovsky, D. Lande, A. Boldak, K. Yefremov, M. Perestyuk // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 69–80.

Abstract. A combined approach has been developed to assess the effectiveness of social transformations as a measure of inconsistency between the actions of the authorities and the expectations of society and the synergy (social activity) of people, based on formalized coordination of the results obtained by the method of expert assessments and methods of sentiment analysis and intelligent analysis of text messages from open online sources and social networks. These methods are implemented as a set of web services and applications in the development environment of the Advanced Analytics integrated online platform of the World Data Center “Geoinformatics and Sustainable Development”. The effectiveness of the proposed approach is demonstrated by the example of a quantitative assessment of the attitude of the population of Ukraine to the actions of the authorities aimed at countering the spread of the COVID-19 epidemic.

Keywords: vector of government actions, vector of society’s expectations, vector of transformations (reforms), linguistic analysis, content analysis, linguistic sentiment analysis of Internet media data and social networks, open source intelligence.

==========

УДК 519.6:517

Оптимальные по точности квадратурные формулы вычисления преобразования бесселя для некоторых классов подынтегральных функций / В.К. Задирака, Л.В. Луц // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 81–95.

Аннотация. Рассмотрена задача построения оптимальных по точности на классах функций и близких к ним квадратурных формул вычисления преобразования Бесселя. Для некоторых классов подынтегральных функций построены оптимальные по точности оценки погрешности вычисления преобразования Бесселя, а также квадратурные формулы, на которых эти оценки достигаются.

Ключевые слова: преобразование Бесселя, оптимальная по точности квадратурная формула, интерполяционные классы функций, метод шапочек, метод граничных функций.

Оптимальні за точністю квадратурні формули обчислення перетворення бесселя для деяких класів підінтегральних функцій / В.К. Задірака, Л.В. Луц // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 81–95.

Анотація. Розглянуто задачу побудови оптимальних за точністю на класах функцій та близьких до них квадратурних формул обчислення перетворення Бесселя. Для деяких класів підінтегральних функцій побудовано оптимальні за точністю оцінки похибки обчислення перетворення Бесселя, а також квадратурні формули, на яких ці оцінки досягаються.

Ключові слова: перетворення Бесселя, оптимальна за точністю квадратурна формула, інтерполяційні класи функцій, метод капелюхів, метод граничних функцій.

Optimal for accuracy quadrature formulas for calculating of the bessel transformation for certain classes of sub-integral functions / V.K. Zadiraka, L.V. Luts // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 81–95.

Abstract. The paper considers the problem of constructing optimal for accuracy in classes of functions and close to them quadrature formulas for calculating the Bessel transformation. For some classes of subintegral functions, optimal estimates of the error in calculating the Bessel transform are constructed, and quadrature formulas are constructed on which these estimates are achieved.

Keywords: Bessel transformation, optimal in accuracy quadrature formula, interpolation classes of functions, hat method, boundary functions method.

==========

УДК 519.2, 519.61, 519.71

Оценка решений переопределенных слау с неточно заданной правой частью / В.Ф. Губарев, Е.А. Шарапов // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 96–109.

Аннотация. Рассмотрены и исследованы методы решения переопределенных СЛАУ, у которых основная матрица известна точно, а правая часть содержит погрешность. Предполагается, что покомпонентная погрешность является случайной величиной, принадлежащей малому ограниченному интервалу. При точных значениях правой части система имеет однозначное решение. В основу развиваемого подхода положено гарантированное оценивание интервалов принадлежности точного решения, по которым можно судить о качестве получаемых приближенных оценок решений. Эти гарантированные оценки используются при сравнении методов и оценивании их эффективности. По результатам численного моделирования сделан сравнительный анализ методов и даны рекомендации по их практическому применению.

Ключевые слова: переопределенные СЛАУ, оценивание, гарантированный интервал, сингулярное разложение, ограниченная погрешность, МНК, обусловленность.

Оцінка розв'язків перевизначених слар з неточно заданою правою частиною / В.Ф. Губарев, Є.О. Шарапов // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 96–109.

Анотація. Розглянуто та досліджено методи розв'язування перевизначених СЛАР, в яких основна матриця відома точно, а права частина містить похибку. Вважається, що покомпонентна похибка є випадковою величиною, яка належить малому обмеженому інтервалу. За точних значень правої частини система має однозначний розв'язок. В основу підходу, що розвивається, покладено гарантоване оцінювання інтервалів належності точного розв'язку, за якими можна робити висновок про якість одержуваних наближених оцінок розв'язків. Ці гарантовані оцінки використовуються для порівняння методів і оцінювання їхньої ефективності. За результатами чисельного моделювання зроблено порівняльний аналіз методів та наведено рекомендації щодо їхнього практичного застосування.

Ключові слова: перевизначені СЛАР, оцінювання, гарантований інтервал, сингулярний розклад, обмежена похибка, МНК, обумовленість.

Solution estimation of overdetermined slae with nonaccurate right side / V.F. Gubarev, Y.A. Sharapov // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 96–109.

Abstract. Methods of overdetermined SLAE solving when main matrix is precise and right side contains errors are considered and studied in the paper. It is assumed that each error of right side component is random but being bounded small interval. Under precise right side system has unique solution. The base of the developed approach is guarantee estimation of interval membership of the precise solution which may be used for quality estimation of the approximate solution. These guarantee estimation are namely applied for comparison and solution quality estimation of the solving methods to be considered. Results of numerical simulation make it possible doing methods comparative analysis and formulation of the recommendations on its practical application.

Keywords: overdetermined SLAE, estimation, guarantee interval, SVD, bounded errors, LSM, conditionality.

==========

УДК 519.2
Точные оценки вероятности попадания неотрицательной унимодальной случайной величины в специальные интервалы при неполной информации / Л.С. Стойкова // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 110–114.

Аннотация. Найдены точные нижние оценки вероятностей попадания неотрицательных унимодальных случайных величин μ в интервалы $(m - \alpha\sigma_\mu, m + \alpha\sigma_\mu)$, где мода m, которая совпадает с первым моментом случайной величины μ, меньше, чем среднее квадратическое отклонение: $m < \sigma_\mu$. Параметр α удовлетворяет неравенствам $0 < \alpha < m / \sigma_\mu < 1$. Этот результат может быть применен при расчете вероятности попадания снаряда в полосу при прицельной стрельбе.

Ключевые слова: линейные функционалы от унимодальных функций распределения, экстремальные значения линейных функционалов, преобразование Джонсона–Роджерса, точные обобщенные неравенства Чебышева для функционалов от унимодальных функций распределения.

Точні оцінки ймовірності попадання невід'ємної унімодальної випадкової величини у спеціальні інтервали за неповної інформації / Л.С. Стойкова // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 110–114.

Анотація. Знайдено точні нижні оцінки ймовірності попадання невід'ємної унімодальної випадкової величини μ в інтервали $(m - \alpha\sigma_\mu, m + \alpha\sigma_\mu)$, де мода m збігається з першим моментом випадкової величини μ і меньше, ніж середнє квадратичне відхилення: $m < \sigma_\mu$. Параметр α задовольняє нерівностям $0 < \alpha < m / \sigma_\mu < 1$. Цей результат можна застосувати для розрахунку ймовірності попадання снаряда в смугу під час прицільної стрільби.

Ключові слова: лінійні функціонали від унімодальної функції розподілу, екстремальні значення лінійних функціоналів, перетворення Джонсона–Роджерса, точні узагальнені нерівності Чебишова для функціоналів від унімодальних функцій розподілу.

Accurate estimates of the probability of a non-negative unimodal random value into special intervals with incomplete information / L.S. Stoikova // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 110–114.

Abstract. Exact lower estimations are found for the probability that non-negative unimodal random variable μ gets in the intervals $(m - \alpha\sigma_\mu, m + \alpha\sigma_\mu)$ where the mode m coincides with fixed first moment of random variable μ, σ_μ is standard deviation and $m < \sigma_\mu$. The parameter α satisfies the inequalities $0 < \alpha < m / \sigma_\mu < 1$. The results of this study may be useful in evaluating the probability of hitting the projectile zone when aimed shooting.

Keywords: linear functionals of distribution functions, their extremal values, transformation of Johnson-Rogers, exact generalized Chebyshoff inequalities for linear functionals of unimodal distribution functions.

==========

УДК 681.3.06:006.354
Стойкость хеш-функции Poseidon к небинарным разностным и линейным атакам / Л.В. Ковальчук, Р.В. Олейников, М.Ю. Родинко // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 115–127.

Аннотация. Построены оценки стойкости хеш-функции Poseidon к небинарным линейным и разностным атакам. Определены общие параметры хеш-функции Poseidon, позволяющие использовать её в рекуррентных SNARK-доказательствах, базирующихся на триплетах MNT-4 и MNT-6. Выполнен анализ того, как нужно выбирать S-блоки для этой хеш-функции, чтобы этот выбор был оптимальным с точки зрения как стойкости, так и количества констрейнтов. Показано, какое количество раундов является достаточным, чтобы гарантировать стойкость этой хеш-функции к небинарным линейным и разностным атакам, вычислено количество констрейнтов на бит информации для предложенных реализаций этой функции с демонстрацией существенного выигрыша в сравнении с хеш-функцией Педерсена.

Ключевые слова: SNARK, констрейнты, хеш-функция Poseidon, небинарный линейный и разностный криптоанализ.

Стійкість геш-функції Poseidon до небінарних різницевих та лінійних атак / Л.В. Ковальчук, Р.В. Олійников, М.Ю. Родінко // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 115–127.

Анотація. Побудовано оцінки стійкості геш-функції Poseidon до небінарних лінійних та різницевих атак. Визначено загальні параметри для геш-функції Poseidon, які забезпечують можливість її використання у рекурентних SNARK-доведеннях, що ґрунтуються на триплетах MNT-4 та MNT-6. Проаналізовано, як потрібно обирати S-блоки для цієї геш-функції, щоб цей вибір був оптимальним з погляду як стійкості, так і кількості констрейнтів. Показано, яка кількість раундів є достатньою, щоб гарантувати стійкість такої геш-функції до небінарних лінійних та різницевих атак, та обчислили кількість констрейнтів на біт інформації для запропонованих реалізацій цієї функції з демонстрацією суттєвого виграшу порівняно з геш-функцією Педерсена.

Ключові слова: SNARK, констрейнти, геш-функція Poseidon, небінарний лінійний та різницевий криптоаналіз.

Security of Poseidon hash function against non-binary differential and linear attacks / L. Kovalchuk, R. Oliynykov, M. Rodinko // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 115–127.

Abstract. In this work we build the security estimations of Poseidon hash function against non-binary linear and differential attacks. We adduce the general parameters for the Poseidon hash function that allow using this hash function in recurrent SNARK-proofs based on MNT-4 and MNT-6 triplets. We also analysed how to choose S-boxes for such function for this choice to be optimal from the point of view of the number of constraints and security. We also showed how many full rounds is sufficient to guarantee security of such hash function against non-binary linear and differential attacks and calculated the number of constraints per bit that is achieved in the proposed realizations demonstrating a considerable gain was demonstrated, as compared to the Pedersen hash function.

Keywords: SNARK, constraints, Poseidon hash function, non-binary linear and differential cryptanalysis.

==========

УДК 519.872

Система обслуживания *GI* / *G* / 1 типа Лакатоша с *T*-возвращением / Е.В. Коба, С.В. Серебрякова // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 128–138.

Аннотация. Рассмотрена система обслуживания *GI* / *G* / 1 типа Лакатоша с *T*-возвращением заявок, т.е. система с *FCFS* дисциплиной обслуживания и постоянным временем *T* цикла орбиты. Для такой системы построена цепь Маркова, доказано условие эргодичности, при определенном соотношении времени обслуживания и времени пребывания на орбите решена система уравнений для стационарного распределения вероятностей состояний системы, выведены формулы для средних показателей количества заявок и количества циклов заявки на орбите. Разработан алгоритм статистического моделирования функционирования системы. Результаты аналитического и статистического моделирования согласуются. Указано важное свойство систем типа Лакатоша: она может применяться для оценки системы, в которой обслуживание с дисциплиной *FCFS* необязательно.

Ключевые слова: системы массового обслуживания с возвращением заявок, система типа Лакатоша, системы с циклическим временем ожидания, система с *T*-возвращением, орбита, цикл орбиты, цепь Маркова, эргодичность системы обслуживания.

Система обслуговування *GI* / *G* / 1 типу Лакатоша з *T*-поверненням / О.В. Коба, С.В. Серебрякова // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 128–138.

Анотація. Розглянуто систему обслуговування *GI* / *G* / 1 типу Лакатоша з *T*-поверненням заявок, тобто систему з *FCFS* дисципліною обслуговування та сталим часом *T* циклу орбіти. Для такої системи побудовано ланцюг Маркова, доведено умову ергодичності, за певного співвідношення часу обслуговування та часу перебування на орбіті розв'язано систему рівнянь для стаціонарного розподілу ймовірностей станів системи, виведено формули для середніх показників кількості заявок та кількості циклів заявки на орбіті. Розроблено алгоритм статистичного моделювання функціонування такої системи. Результати аналітичного та статистичного моделювання узгоджуються. Вказано важливу властивість систем типу Лакатоша: вона може застосовуватися для оцінювання системи, у якій не обов'язкове обслуговування за дисципліною *FCFS*.

Ключові слова: системи масового обслуговування з поверненням заявок, система типу Лакатоша, системи з циклічним часом очікування, система з *T*-поверненням, орбіта, цикл орбіти, ланцюг Маркова, ергодичність системи обслуговування.

***GI* / *G* / 1 Lakatos-type queueing system with *T*-retrials / O.V. Koba, S.V. Serebriakova** // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 128–138.

Abstract. Authors consider the Lakatosh-type T queueing system with T-retrials, i.e., the system with the FCFS service discipline and a constant cycle time T of the orbit. Here we construct the Markov chain for the system, prove its ergodicity condition, solve the system of equations for the stationary distribution of the system state probabilities, and derive formulas for the average number of requests and the average number of the orbit cycles at a specific ratio of service time and orbit time. Also, we develop an algorithm for statistical modeling of the considered system. Results of analytical and statistical modeling show consistency between them. Authors indicate an essential property of the Lakatos-type system, namely, that we can use it to evaluate a system in which the FCFS service order is not necessary.

Keywords: retrial queues, Lakatos-type queueung system, cyclic queueing systems, queueing system with *T*-retrials, orbit, orbit cycle, Markov chain, queueing system ergodicity.

==========

УДК 519.8

Оптимальные быстродействия в управляемой системе Лотки–Вольтерры / С.В. Пашко // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 139–146.

Аннотация. Рассматривается управляемая система дифференциальных уравнений Лотки–Вольтерры, описывающая процесс развития двух взаимосвязанных популяций хищников и жертв. Система содержит две переменные управления, которые выбираются так, чтобы время перехода к стационарной точке было минимальным. Построены функции управления и соответствующие траектории движения в фазовом пространстве и обоснована их оптимальность.

Ключевые слова: принцип максимума, стационарная точка, минимальное время.

Оптимальні швидкодії в керованій системі Лотки–Вольтерри / С.В. Пашко // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 139–146.

Анотація. Розглянуто керовану систему диференціальних рівнянь Лотки–Вольтерри, що описує процес розвитку двох взаємопов'язаних популяцій хижаків та жертв. Система містить дві змінні керування, які обирають так, щоб час переходу до стаціонарної точки був мінімальним. Побудовано функції керування і відповідні траєкторії руху в фазовому просторі та обгрунтовано їхню оптимальність.

Ключові слова: принцип максимуму, стаціонарна точка, мінімальний час.

Time optimal control problem for the Lotka–Volterra system / S.V. Pashko // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 139–146.

Abstract. We consider a controlled system of Lotka–Volterra differential equations that describes the evolution of two interrelated populations of predators and prey. The system contains two control variables, which are chosen so that the transition time to a stationary point is minimal. In the article, the control functions and the corresponding trajectories of motion in the state space are constructed, and their optimality is substantiated.

Keywords: maximum principle, stationary point, minimum time.

==========

УДК 517.977

Метод разрешающих функций для игровых задач сближения управляемых объектов с различной инерционностью / И.С. Раппопорт // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 147–166.

Аннотация. Рассмотрена проблема сближения управляемых объектов с различной инерционностью в игровых задачах динамики на основе современной версии метода разрешающих функций. Для таких объектов характерно, что на некотором интервале времени не выполняется условие Понтрягина, что существенно затрудняет применение метода разрешающих функций к этому классу игровых задач динамики. Предложен метод решения таких задач, связанный с построением некоторых скалярных функций (разрешающих), качественно характеризующих ход сближения управляемых объектов с различной инерционностью и эффективность принятых решений. Метод разрешающих функций позволяет эффективно использовать современную технику многозначных отображений в обоснованиях игровых конструкций и получении на их основе содержательных результатов. Сравниваются гарантированные времена окончания игры для разных схем сближения управляемых объектов. Приведен иллюстративный пример.

Ключевые слова: управляемые объекты с различной инерционностью, квазилинейная дифференциальная игра, многозначное отображение, измеримый селектор, стробоскопическая стратегия, разрешающая функция.

Метод розв'язувальних функцій для ігрових задач зближення керованих об'єктів з різною інерційністю / Й.С. Раппопорт // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 147–166.

Анотація. Розглянуто проблему зближення керованих об'єктів з різною інерційністю в ігрових завданнях динаміки на основі сучасної версії методу розв'язувальних функцій. Для таких об'єктів характерно, що на деякому інтервалі часу не виконується умова Понтрягіна, що істотно ускладнює застосування методу розв'язувальних функцій до цього класу ігрових задач динаміки. Запропоновано метод розв'язання таких задач, пов'язаний з побудовою деяких скалярних функцій (розв'язувальних), що якісно характеризують хід зближення керованих об'єктів з різною інерційністю та ефективність прийнятих рішень. Метод розв'язувальних функцій дає змогу ефективно використовувати сучасну техніку багатозначних відображень в обгрунтуваннях ігрових конструкцій і отриманні на їхній основі змістовних результатів. Порівнюються гарантовані часи закінчення гри для різних схем зближення керованих об'єктів. Наведено ілюстративний приклад.

Ключові слова: керовані об'єкти з різною інерційністю, квазілінійна диференціальна гра, багатозначне відображення, вимірний селектор, стробоскопічна стратегія, розв'язувальна функція.

Resolving functions method for game problems of releaseof controlled objects with different inertia / I.S. Rappoport // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 147–166.

Abstract. The problem of convergence of controlled objects with different inertia in game dynamics problems is considered on the basis of the modern version of the method of resolving functions. For such objects, it is characteristic that the Pontryagin condition is not satisfied on a certain time interval, which significantly complicates the application of the method of resolving functions to this class of game dynamics problems. A method for solving such problems is proposed, which is associated with the construction of some scalar functions (resolving), which qualitatively characterize the course of con vergence of controlled objects with different inertia and the efficiency of the decisions made. The method of resolving functions is that it allows you to effectively use the modern technique of multivalued mappings in substantiating game constructions and obtaining meaningful results based on them. The guaranteed end times of the game are compared for different schemes of approaching controlled objects. An illustrative example is given.

Keywords: controlled objects with different inertia, quasilinear differential game, multi-valued mapping, measurable selector, stroboscopic strategy, resolving function.

УДК 355.41

Логистическое дифференциальное уравнение в частных производных для определения рационального размещения и изменения объемов запасов материальных средств / А.И. Хазанович, М.А. Кудрицкий // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 167–169.

Аннотация. Выведено логистическое дифференциальное уравнение в частных производных для определения рационального размещения и изменения объемов запасов материальных средств в течение периода обеспечения. В дальнейшем с использованием логистического дифференциального уравнения в частных производных можно определять и рассчитывать конкретные значения показателей, входящих в решение логистического дифференциального уравнения в частных производных.

Ключевые слова: логистическое дифференциальное уравнение, запасы материальных средств.

Логістичне диференціальне рівняння у частинних похідних для визначення раціонального розміщення та зміни обсягів запасів матеріальних засобів / О.І. Хазанович, М.О. Кудрицький // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 167–169.

Анотація. Виведено логістичне диференціальне рівняння у частинних похідних для визначення раціонального розміщення та зміни обсягів запасів матеріальних засобів протягом періоду забезпечення. Надалі з використанням логістичного диференціального рівняння у частинних похідних можна визначати та обчислювати конкретні значення показників, що входять до розв'язку логістичного диференціального рівняння у частинних похідних.

Ключові слова: логістичне диференціальне рівняння, запаси матеріальних засобів.

Logistic differential equation in partial derivatives for determination of rational location and changes in inventories of materials / O.I. Khazanovych, M.O. Kudrytskyi // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 167–169.

Abstract. In the article, it is deduced the logistic differential equation in partial derivatives to determine the rational placement and change in the inventories of material means during the provision period. In the future, using the logistic differential equation in partial derivatives, it is possible to determine and calculate the specific values of indicators that are part of the solution of the logistic differential equation in partial derivatives.

Keywords: logistic differential equation, inventories of material means.

==========

ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ SOFTWARE–HARDWARE COMPLEXES

УДК 519.6

Высокопроизводительные суперкомпьютерные технологии моделирования и идентификации сложных нанопористых киберсистем с обратными связями для *n*-компонентной компетитивной адсорбции / М.Р. Петрик, И.В. Бойко, А.Н. Химич, М.М. Петрик // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 170–183.

Аннотация. Разработаны высокопроизводительные суперкомпьютерные технологии вычислений для моделирования и идентификации параметров сложных процессов *n*-компонентной компетитивной адсорбции в нанопористых киберсистемах с обратными связями. Предложено эффективное распараллеливание векторных составляющих решения модели с использованием преобразования Лапласа и операционного метода Хевисайда и декомпозицией нелинейной системы с условиями адсорбционного равновесия типа Ленгмюра. Представлены результаты численных экспериментов на основе параллельных вычислений с использованием многоядерных компьютеров.

Ключевые слова: высокопроизводительные параллельные вычисления, нанопористые киберсистемы с обратными связями, компететивна адсорбция газов, функция адсорбционного равновесия Ленгмюра, интегральное преобразование Лапласа, операционный метод Хевисайда.

Високопродуктивні суперкомп'ютерні технології моделювання та ідентифікації складних нанопористих кіберсистем зі зворотними зв'язками для *n*-компонентної компетитивної адсорбції / М.Р. Петрик, І.В. Бойко, О.М. Хіміч, М.М. Петрик // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 170–183.

Анотація. Розроблено високопродуктивні суперкомп'ютерні технології обчислень для моделювання та ідентифікації параметрів складних процесів *n*-компонентної компетитивної адсорбції в нанопористих кіберсистемах зі зворотними зв'язками. Запропоновано ефективне розпаралелювання векторних складовихт розв'язку моделі з використанням перетворення Лапласа та операційного методу Гевісайда з декомпозицією нелінійної системи з умовами адсорбційної рівноваги типу Ленгмюра. Наведено результати числових експериментів на основі паралельних обчислень з використанням багатоядерних комп'ютерів.

Ключові слова: високопродуктивні паралельні обчислення, нанопористі кіберсистеми зі зворотними зв'язками, компетитивна адсорбція газів, функція адсорбційної рівноваги Ленгмюра, інтегральне перетворення Лапласа, операційний метод Гевісайда.

High-performance supercomputer technologies of simulation and identification of nanoporous systems with feedback for n-component competitive adsorption / **M.R. Petryk, I.V. Boyko, O.M. Khimich, M.M. Petryk** // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 170–183.

Abstract. High-performance supercomputer computing technologies have been developed to model and identify the parameters of complex n-component competitive adsorption processes in nanoporous cybersystems with feedback. Using the Laplace transform and the Heaviside operating method with the decomposition of a nonlinear system with Langmuir-type adsorption equilibrium conditions, an effective parallelization of the vector components of the model solution is proposed. The results of numerical experiments based on parallel computations using multi-core computers are presented.

Keywords: high-performance parallel computations, nanoporous cybersystems with feedback, competent gas adsorption, Langmuir adsorption equilibrium function, Laplace integral transformation, Heaviside operating method.

==========

УДК 004.056.55

Симметричные криптоалгоритмы в системе остаточных классов / М.Н. Касянчук, И.З. Якименко, Я.Н. Николайчук // Кибернетика и системный анализ. 2021. Том 57, № 2. С. 184–192.

Аннотация. Представлены теоретические основы симметричного шифрования на основе системы остаточных классов. Особенности этого подхода заключаются в том, что при восстановлении десятичного числа по его остаткам с использованием китайской теоремы об остатках умножения осуществляются на произвольно выбранные коэффициенты (ключи). Установлено, что криптостойкость разработанных методов определяется количеством модулей и их разрядностью. Отмечено, что описанные методы позволяют практически неограниченно увеличивать блок открытого текста для шифрования, что устраняет необходимость использования различных режимов шифрования.

Ключевые слова: система остаточных классов, криптоалгоритм, симметричная криптосистема, шифртекст, криптоанализ, устойчивость.

Симетричні криптоалгоритми у системі залишкових класів / М.М. Касянчук, І.З. Якименко, Я.М. Николайчук // Кібернетика та системний аналіз. 2021. Том 57, № 2. С. 184–192.

Анотація. Представлено теоретичні основи симетричного шифрування на основі системи залишкових класів. Особливості цього підходу полягають у тому, що у випадку відновлення десяткового числа за його залишками з використанням китайської теореми про залишки множення здійснюється на довільно вибрані коефіцієнти (ключі). Встановлено, що криптостійкість розроблених методів визначається кількістю модулів та їхньою розрядністю. З'ясовано, що описані методи забезпечують можливість практично необмеженого збільшення блоку відкритого тексту для шифрування, при цьому зникає потреба у використанні різних режимів шифрування.

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

Symmetric cryptoalgorithms in the residue number system / M.M. Kasianchuk, I.Z. Yakymenko, Ya.M. Nykolaychuk // Kibernetika i sistemnyj analiz. 2021. Vol. 57, N 2. P. 184–192.

Abstract. This paper presents the theoretical backgrounds of symmetric encryption based on a residue number system. The peculiarities of this approach include that when restoring a decimal number to its residuals appears using the Chinese remainder theorem, multiplication occurs by arbitrarily chosen coefficients (keys). It is established that cryptostability of the developed methods is determined by the number of modules and their bit size. In addition, the described methods allow almost indefinitely increase the block of plain text for encryption, which eliminates the need to use different encryption modes.

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