КІБЕРНЕТИКА **CYBERNETICS**

УДК 519.7

Теоретичні основи аналітичного обчислення коефіцієнтів базисних чисел перетворення Крестенсона / Николайчук Я.М., Касянчук М.М., Якименко І.З. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 3–8.

Представлено теоретичні основи аналітичного обчислення коефіцієнтів базисних чисел перетворення Крестенсона, що істотно зменшує кількість операцій, необхідних для переведення чисел з системи залишкових класів у десяткову систему числення. При цьому відповідний підбір модулів дозволяє досягнути ефективного використання усіх регістрів розрядної сітки. Іл.: 1. Табл.: 1. Бібліогр.: 15 назв.

UDC 519.7

Theoretical foundations for the analytical calculation of the coeficients of basic numbers of Krestenson's transformation / Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 3–8.

The paper presents the theoretical foundations for the analytical transformation of coefficients of basic numbers of Krestenson's transformation, which significantly reduces the number of operations required to convert from residue number system to decimal one. The appropriate selection of modules allows the efficient use of all the word length registers. Fig.: 1. Tabl.: 1. Refs: 15 titles.

УДК 510.23+510.25+510.54+512.567

Конструктивно-продукційні структури та їх граматичні інтерпретації. I. Узагальнена формальна конструктивно-продукційна структура / Шинкаренко В.І., Ільман В.М. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 8–16.

Узагальнено можливості різних модифікацій формальних граматик, запропоновано апарат конструктивно-продукційних структур, що дозволяє формалізувати процеси і результати формування конструкцій на основі елементів з атрибутами. Розглянуто можливості спеціалізації, конкретизації конструктивно-продукційних структур, а також інтерпретації на основі алгоритмічних структур, які моделюють виконавця. Бібліогр.: 21 назва.

UDC 510.23+510.25+510.54+512.567

Constructive-synthesizing structures and their grammatical interpretations. I. Generalized formal constructive-synthesizing structure / Shynkarenko V.I., Ilman V.M. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 8–16.

Various modifications of formal grammars are summarized. The constructive-synthesizing structure framework is proposed. Its tools make it possible to formalize the processes and results of construction formation using the basis of elements with attributes. The possibilities of specialization, specification of constructive-synthesizing structures, and interpretation based on algorithmic structures that simulate an executor are considered. Refs: 21 titles.

СИСТЕМНИЙ АНАЛІЗ **SYSTEMS ANALYSIS**

УДК 519.217.2

Стійкість генетичного коду до точкових мутацій / Сергієнко І.В., Гупал А.М., Островський О.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 17–24.

Досліджено стійкість генетичних кодів при мутаціях в нуклеотидах. Проведено порівняння універсального коду з кодами, що випадково згенерували. Досліджено стійкість генетичного коду щодо таких характеристик амінокислот, як полярність, гідрофобність і схильність до утворення спіралей. Описано генетичний алгоритм для оптимізації стійкості коду. Табл.: 6. Бібліогр.: 9 назв.

UDC 519.217.2

Noise immunity of genetic code to point mutations / Sergienko I.V., Gupal A.M., Ostrovskii A.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 17–24.

The noise immunity of genetic codes with nucleotide mutations is analyzed. A universal code is compared with randomly generated codes. The noise immunity of genetic code against polarity, hydrophoby, and helix propensity is analyzed. A genetic algorithm for the optimization of noise immunity code is described. Tabl.: 6. Refs: 9 titles.

УДК 519.6

Явні формули для інтерполяційних сплайнів 5-го степеня на трикутнику / Сергієнко І.В., Литвин О.М., Литвин О.О., Денисова О.І. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 25–33.

Побудовані явні формули для 21 базисного інтерполяційного полінома 5-го степеня Зламала–Женішека у кожному трикутнику тріангуляції. Їх використання дозволяє значно зменшити кількість арифметичних операцій в МСЕ, оскільки без вказаних базисних функцій треба розв'язувати в кожному трикутнику двадцять одну систему з 21 невідомою для знаходження всіх 21 коефіцієнта кожного базисного інтерполяційного полінома 5-го степеня. Наведено також формулу для операторів інтерполяції з використанням вказаних базисних поліномів і формулу для інтегрального представлення залишкового члена наближення диференційовних функцій вказаними операторами. Бібліогр.: 30 назв.

UDC 519.6

Explicit formulas for interpolation splines of degree 5 on the triangle / Sergienko I.V., Lytvyn O.M., Lytvyn O.O., Denisova O.I. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 25–33.

Explicit formulas are given for 21 Zlámal–Zenishek base interpolation polynomials of 5th degree in each triangle of the triangulation. Their use can significantly reduce the number of arithmetic operations in the FEM, because otherwise 21 systems with 21 unknowns should be solved in each triangle to find all the 21 coefficients of each of the base interpolation polynomials of 5th degree. The formulas are also presented for interpolation operators with the use of these base polynomials and for the integral representation of the remainder term of the approximation of differentiable functions by these operators. Refs: 30 titles.

УДК 519.856

Зведення задач двоетапної ймовірнісної оптимізації з дискретним розподілом випадкових даних до задач частково цілочисельного програмування / Норкін В.І., Кібзун А.І., Наумов А.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 34–48.

Розглянуто моделі двоетапного стохастичного програмування з квантильним критерієм, а також моделі з імовірнісним обмеженням на випадкові значення цільової функції другого етапу. Такі моделі дозволяють формалізувати вимоги до надійності і безпеки системи, що оптимізується, а також оптимізувати її функціонування в екстремальних умовах. Запропоновано спосіб еквівалентного перетворення моделей при дискретному розподілі випадкових параметрів до задач частково цілочисельного програмування. Число додаткових цілочисельних (булевих) змінних в цій задачі дорівнює числу можливих значень вектора випадкових параметрів. Отримані змішані задачі розв'язуються за допомогою потужних стандартних комп'ютерних програм дискретної оптимізації. Наведено результати чисельного експерименту на задачі невеликої вимірності. Бібліогр.: 35 назв.

UDC 519.856

Reducing two-stage probabilistic optimization problems with discrete distribution of random data to mixed-integer programming problems / Norkin V.I., Kibzun A.I., Naumov A.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 34–48.

We consider a two-stage stochastic programming model with quantile criterion, as well as models with a probabilistic constraint on the random value of the objective function of the second stage. These models allow us to formalize the requirements for the reliability and safety of the system being optimized and to optimize the system performance under extreme conditions. We propose a method of equivalent transformation of these models under discrete distribution of random parameters to mixed-integer programming problems. The number of additional integer (Boolean) variables in these problems equals to the number of possible values of the vector of random parameters. The obtained mixed optimization problems can be solved by powerful standard discrete optimization software. To illustrate the approach, the results of numerical experiment for the problem of small dimension are presented. Refs: 35 titles. Refs: 35 titles.

УДК 519.8

Моделі і складність задач проектування та реконструкції телекомунікаційних і транспортних систем / Шаріфов Ф.А., Гуляницький Л.Ф. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 49–58.

Розглянуто проблеми синтезу мереж, які виникають при проектуванні і експлуатації телекомунікаційних та транспортних мереж. Запропоновано формалізацію задач синтезу мереж на графах, в яких задано обмеження на пропускні здатності розрізів і враховуються можливості виходу з ладу деяких компонентів мережі. Описано підходи до розв`язання та аналізу трудомісткості задач, що виникають. Бібліогр.: 23 назви.

UDC 519.8

Models and complexity of the design and reconstruction of telecommunication and transportation systems / Sharifov F.A., Hulianytskyi L.F. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 49–58.

We address network synthesis problems arising in the design and exploitation of telecommunication and transportation systems. We focus on the formulations of the network design problems on graphs with bounded capacities of cuts and connectivity requirements after some network components fail. We discuss the approaches to problem solutions and analyze their run times. Refs: 23 titles.

УДК 517.9, 519.816

Гібридний метод багатокритеріального оцінювання альтернатив прийняття рішень / Панкратова Н.Д., Недашківська Н.І. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 58–70.

Розроблено гібридний метод підтримки прийняття рішень при залежних критеріях рішень, що включає методи теорії прийняття рішень, нечітких множин, математичного програмування і статистики, які адаптуються на різних етапах багатокритеріального оцінювання альтернатив залежно від конкретної розв'язуваної задачі і якості вхідної експертної інформації. Проілюстровано використання гібридного методу при вирішенні практичного завдання. Іл.: 1. Табл.: 4. Бібліогр.: 27 назв.

UDC 517.9, 519.816

Hybrid method of multicriteria evaluation of decision-making alternatives / Pankratova N.D., Nedashkivska N.I. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 58–70.

In the paper we develop a hybrid decision support method in case of dependent solution criteria. It includes the methods of decision theory, fuzzy sets, mathematical programming and statistics, which are adapted to different stages of the multicriteria evaluation of alternatives depending on the specific problem being solved and on the quality of the input of expert information. The use of the hybrid method is illustrated by the solution of practical problems. Fig.: 1. Tabl.: 4. Refs: 27 titles.

УДК 519.8

Властивості збурених конусів, упорядковуючих множину допустимих розв'язків векторної оптимізаційної задачі / Лебєдєва Т.Т., Семенова Н.В., Сергієнко Т.І. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 71–77.

Досліджено вплив збурень у вхідних даних на розв'язки векторної оптимізаційної задачі з багатьма лінійними критеріями. Проведено аналіз властивостей збурених конусів, що частково впорядковують множину допустимих розв'язків задачі векторної оптимізації відносно лінійних цільових функцій. Вивчено структуру всієї сукупності спеціальним чином збурених упорядковуючих конусів, що відповідають різним значенням параметра збурень вхідних даних задачі. Бібліогр.: 10 назв.

UDC 519.8

Properties of perturbed cones that order the feasible domain of vector optimization problem / Lebedeva T.T., Semenova N.V., Sergienko T.I. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 71–77.

The influence of perturbations of the initial data on the solutions of multicriteria optimization problems is considered. The properties of perturbed cones, which partially order the feasible domain of the vector optimization problem with respect to the linear objective functions are analyzed. The structure of the set of specific perturbed ordering cones with different values of the parameter of perturbations of initial data is investigated. Refs: 10 titles.

УДК 519.81

Методи комплексування даних / Воронін А.М. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 78–84.

Розглянуто методи комплексування даних, що дозволяють при обмеженому числі каналів отримувати максимально можливу кількість доступної інформації. Поряд з концепцією редукторів ступенів свободи пропонується застосовувати підхід дискримінаторів ступенів свободи, що дає змогу усім каналам, в міру їх інформативності в поточній ситуації, приймати участь у виробленні кооперативного рішення. Бібліогр.: 14 назв.

UDC 519.81

Data complexation methods / Voronin A.N. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 78–84.

The methods of data complexation are proposed. For a limited number of channels, they allow obtaining the maximum possible amount of available information. Along with the reducers of degrees of freedom, discriminators of degrees of freedom are proposed to be used, which enables all the channels, in accordance with their current informativeness, to take part in making a cooperative decision. Refs: 14 titles.

УДК 519.21

Поліедральні когерентні міри ризику і оптимальні портфелі за співвідношенням винагорода–ризик / Кирилюк В.С. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 85–103.

Досліджено проблеми пошуку оптимальних портфельних рішень за співвідношенням винагорода–ризик в умовах ризику і часткової невизначеності. Показано, яким чином подібні проблеми зводяться до задач лінійного програмування як у випадку відомих розподілів випадкових величин, так і у випадку неточних ймовірностей сценаріїв. Розглянуто набір прикладів застосування. Бібліогр.: 31 назва.

UDC 519.21

Polyhedral coherent risk measures and optimal portfolios on the reward–risk ratio / Kirilyuk V.S. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 85–103.

The problems of finding the optimal portfolio decisions on the reward–risk ratio under conditions of risk and partial uncertainty are analyzed. It is shown how such problems can be reduced to linear programming problems, both in the case of known distributions of random variables and in the case of imprecise probabilities of scenarios. A set of application examples is considered. Refs: 31 titles.

УДК 517.988

Гібридні методи розщеплення для системи операторних включень з монотонними операторами / Семенов В.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 104–112.

Запропоновано нові алгоритми для розв'язання системи операторних включень з монотонними операторами, що діють в гільбертовому просторі. Алгоритми базуються на трьох відомих методах: алгоритмі розщеплення Ценга та двох гібридних алгоритмах для апроксимації нерухомих точок нерозтягуючих операторів. Доведено теореми про сильну збіжність породжених алгоритмами послідовностей. Бібліогр.: 40 назв.

UDC 517.988

Hybrid splitting methods for the system of operator inclusions with monotone operators / Semenov V.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 104–112.

New algorithms are proposed to solve a system of operator inclusions with monotone operators acting in a Hilbert space. The algorithms are based on three well-known methods: the Tseng forward-backward splitting algorithm and two hybrid algorithms for approximation of fixed points of nonexpansive operators. Theorems on the strong convergence of the sequences generated by the algorithms are proved. Refs: 40 titles.

УДК 519.21

Виведення рівняння для ймовірності небанкрутства страхової компанії, що працює на (B, S)-ринку. Стохастичні позови та стохастичні премії / Бондарев Б.В., Болдирєва В.О. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 113–121.

Для моделі Крамера–Лундберга зі стохастичними преміями виведено інтегро-диференціальні рівняння для ймовірності небанкрутства на скінченному та нескінченному інтервалах часу функціонування страхової компанії, що працює на (B, S)-ринку. Для виведення рівнянь не вимагається існування гладких щільностей розподілу страхових премій та вимог. Бібліогр.: 9 назв.

UDC 519.21

Deriving the equation for the survival probability of the insurance company in (B, S)-market. Stochastic claims and stochastic premiums / Bondarev B.V., Boldyreva V.O. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 113–121.

The integral-differential equations for the survival probability, on finite and infinite time intervals, for the insurance company operating in the (B, S)-market are derived for the Cramer–Lundberg model with stochastic premiums. To derive the equations, smooth distribution densities of premiums and claims are not required. Refs: 9 titles.

УДК 519.168

Двокритеріальний лексикографічній алгоритм побудови усіх найкоротших шляхів у мережі / Васянін В.О. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 122–131.

Розглянуто алгоритм побудови найкоротших шляхів між усіма парами вузлів у неорієнтованій мережі за критерієм: мінімум дуг у шляху; мінімум довжини шляху. Проведено аналіз складності алгоритму та емпірично показано, що в міру зростання щільності мережі його обчислювальна ефективність стає на кілька порядків вищою, ніж у алгоритму Флойда, відповідно модифікованого для відшукання найкоротших шляхів за ступінчатим критерієм. Іл.: 3. Бібліогр.: 12 назв.

UDC 519.168

Two-criterion lexicographic algorithm of finding all shortest paths in networks / Vasyanin V.A. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 122–131.

The algorithm of finding all shortest paths in undirected network is considered. Two criteria are used: the minimum number of arcs in the path and minimum path length. The algorithm is analyzed for complexity and it is empirically shown that as the network density increases, the computational efficiency of the proposed algorithm becomes higher than that of the Floyd algorithm adequately modified to find the shortest path by two criteria. Figs: 3. Refs: 12 titles.

УДК 681.3

Проблеми захисту персональних даних у випадку використання хмарних обчислень / Фаль О.М., Козак В.Ф. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 132–138.

Проведено аналіз використання хмарних обчислень з точки зору виконання вимог захисту персональних даних. Розглянуто рекомендації постачальникам та споживачам хмарних послуг стосовно реалізації принципів оброблення персональних даних. Сформульовано окремі положення проекту міжнародного стандарту щодо захисту персональних даних у хмарах. Бібліогр.: 14 назв.

UDC 681.3

Personal data protection problems when using cloud computing / Fal' O.M., Kozak V.F. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 132–138.

Cloud computing is analyzed with regard to personal data protection. Recommendations to cloud providers and cloud customers as to implementing the principles of personal data processing are discussed. Some provisions of the international standard project concerning personal data protection are formulated. Refs: 14 titles.

УДК 519.21

Стохастичне оптимальне керування процесами ризику з ліпшицевими функціями виграшу / Норкін Б.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 139–154.

Досліджено задачу стохастичного оптимального керування дивідендною політикою страхової компанії в дискретному часі з загальною ліпшицевою функцією виграшу, що включає індикатори прибутковості і ризику. Для побудови позиційних оптимальних керувань та оцінки показників функціонування компанії обґрунтовано метод динамічного програмування. Отримано оцінки швидкості збіжності методу послідовних наближень для знаходження необмежених функцій Беллмана. Парето-оптимальна множина задачі чисельно апроксимується за допомогою бар'єрно-пропорційних стратегій керування. Іл.: 1. Бібліогр.: 34 назви.

UDC 519.21

Stochastic optimal control of risk processes with Lipschitz payoff functions / Norkin B.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 139–154.

The paper studies stochastic optimal control problems for finding optimal dividend policies of an insurance company in discrete time and with general Lipschitz payoff functions, involving indicators of profitability and risk. To construct positional optimal controls and to evaluate performance indicators, the dynamic programming method is validated. The rate of convergence of the successive approximation method for finding generally unbounded Bellman functions is estimated. The Pareto-optimal set of the problem is numerically approximated by so-called barrier-proportional control strategies. Fig.: 1. Refs: 34 titles.

УДК 519.6

Оцінки точності різницевих схем для одновимірного параболічного рівняння з урахуванням впливу початкових і крайових умов / Майко Н.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 154–163.

Отримано оцінки з вагою для точності методу сіток розв'язування початково-крайової задачі для одновимірного параболічного рівняння у випадку мішаної крайової умови (умови Діріхле та Неймана). Показано, що у просторово-часовому прямокутнику порядок точності методу вищий ближче до дна і бічної сторони, на якій задано крайову умову Діріхле. Бібліогр.: 6 назв.

UDC 519.6

The initial and boundary effect in the error estimates of the finite-difference scheme for a one-dimensional parabolic equation / Mayko N.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 154–163.

We obtain the error estimates of the finite-difference scheme for the one-dimensional heat equation, which take into account the influence of the initial and boundary conditions. We prove that the accuracy order is higher near the bottom and the Dirichlet boundary-value side of the time-dimensional rectangle. Refs: 6 titles.

УДК 519.6:539.3

Чисельне розв'язання обернених задач термопружності для складеного циліндра / Аралова А.А. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 164–172.

Проведено аналіз термопружного стану складеного циліндра. Представлено класичні узагальнені задачі, визначені на класах розривних функцій, отримано вирази градієнтів нев'язок у явному вигляді (за допомогою розв'язання прямих та спряжених задач) для реалізації градієнтних методів Аліфанова, шляхом використання функцій методу скінченних елементів побудовано розрахункові схеми підвищеного порядку точності чисельної дискретизації прямих та спряжених задач. Представлено результати деяких модельних прикладів. Табл.: 1. Бібліогр.: 14 назв.

UDC 519.6:539.3

Numerical solution of inverse problems of thermoelasticity for composite cylinder / Aralova A.A. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 164–172.

The thermoelastic state of a composite cylinder is analyzed. The classical generalized problems defined on classes of discontinuous functions are presented. The explicit expressions are obtained for residual gradients (using the solution of direct and adjoint problems) for the implementation of Alifanov's gradient methods; the functions of finite element method are used to construct highly accurate computation schemes for the numerical sampling of direct and adjoint problems. The numerical results for some model examples are presented. Tabl.: 1. Refs: 14 titles.

НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ І СИСТЕМНОГО АНАЛІЗУ

NEW TOOLS IN CYBERNETICS, COMPUTER SCIENCE, AND SYSTEM ANALYSIS

УДК 519.633; 536.252

Побудова вагових функцій методу Петрова–Гальоркіна для рівнянь конвекції–дифузії–реакції у тривимірному випадку / Сальніков М.М., Сірик С.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 173–183.

Запропоновано спосіб побудови неперервних кусково-поліноміальних вагових функцій для методу Петрова–Гальоркіна в тривимірній області. Вид та форма функцій визначені скінченною кількістю параметрів, що пов'язані з ребрами сітки розбиття і якими можна варіювати. Вибором цих параметрів можна отримати чисельні апроксимації для вихідної задачі, в якій відсутні нефізичні осциляції (при збереженні достатньої точності). Результати дослідження проілюстровано декількома чисельними прикладами. Іл.: 1. Бібліогр.: 31 назва.

UDC 519.633; 536.252

Construction of weight functions of the Petrov–Galerkin method for convection–diffusion–reaction equations in three–dimensional case / Salnikov N.N., Siryk S.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 173–183.

We propose a method for constructing a continuous piecewise-polynomial weight functions for the Petrov–Galerkin method in three-dimensional domain. The form of the functions is determined by a finite number of variable parameters associated with the edges of the grid partition. It is expected that the choice of these parameters allows obtaining the numerical approximation of the original equation without non-physical oscillations (when saving the sufficient accuracy). The investigation results are illustrated with some test calculations. Figs: 8. Refs: 31 titles.

СТИСЛІ ПОВІДОМЛЕННЯ

BRIEF COMMUNICATIONS

УДК 512.54.05

Вразливість в квантовій моделі обчислень криптопримітивів, що базуються на задачі пошуку елемента спряження та степеня / Фесенко А.В. // Кибернетика и системный анализ. — 2014. — Том 50, № 5. — С. 184–186.

Розроблено ефективний алгоритм розв'язання в квантовій моделі обчислень узагальненої задачі дискретного логарифмування за допомогою зведення до абелевої задачі про приховану підгрупу. Запропонований метод дозволяє в квантовій моделі обчислень ефективно розв'язати часткову задачу пошуку елемента спряження та степеня, на складності розв'язання якої в деяких групах грунтується стійкість декількох криптографічних систем та протоколів. Бібліогр.: 5 назв.

UDC 512.54.05

Vulnerability in quantum computation model of cryptographic primitives based on the power conjugacy search problem / Fesenko A.V. // Kibernetika i sistemny analiz. — 2014. — Vol. 50, N 5. — P. 184–186.

The paper shows the existence of an efficient algorithm to solve the generalized discrete logarithm problem in quantum computing model by reducing it to the Abelian hidden subgroup problem. The proposed method can also efficiently solve the power conjugacy search subproblem in quantum computing model, on whose complexity in some groups the resistance of several cryptographic systems and protocols is based. Refs: 5 titles.