КІБЕРНЕТИКА **CYBERNETICS**

УДК 519.686.2

Анализ структуры атрибутных транзиционных систем без скрытых переходов / **В.В. Скобелев** // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 3–15.

Іл.: 0. Табл. 0. Бібліогр.: 11 назв.

Проведен теоретико-множественный анализ структуры атрибутных транзиционных систем без скрытых переходов. Предложены частичные операции композиции историй и трасс. Показана возможность их применения для распараллеливания построения покрытий множеств историй и трасс. Определены отношения эквивалентности на множестве состояний. В терминах систем с выделенными начальными и финальными состояниями, а также систем с выделенными начальными состояниями и множествами финальных предельных множеств состояний определены классы безопасных и корректных систем. Построена алгебра таких систем.

Ключевые слова: атрибутные транзиционные системы без скрытых переходов и их композиции, безопасность и корректность, структура множеств состояний, историй и трасс.

Аналіз структури атрибутних транзиційних систем без прихованих переходів / В.В. Скобелєв // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 3–15.

Проведено теоретико-множинний аналіз структури атрибутних транзиційних систем без прихованих переходів. Запропоновано часткові операції композиції історій і трас. Показано можливість їхнього застосування для розпаралелювання побудови покриттів множин історій та трас. Визначено відношення еквівалентності на множині станів. У термінах систем із заданими початковими і фінальними станами, а також систем з заданими початковими станами і множинами фінальних граничних множин станів визначено класи безпечних і коректних систем. Побудовано алгебру таких систем.

Ключові слова: атрибутні транзиційні системи без прихованих переходів та їхні композиції, безпека та коректність, структура множин станів, історій та трас.

Analysis of the structure of attributed transition systems without hidden transitions / V.V. Skobelev // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 3–15.

The paper carries out set-theoretic analysis of the structure of attributed transition systems without hidden transitions. Partial operations of composition of histories and traces are proposed. It is shown that they can be used to parallelize the design of coverings of sets of histories and traces. Equivalence relations on the set of states are extracted. In terms of systems with distinguished initial and final states, as well as systems with distinguished initial states and sets of final limit sets of states, classes of safe and correct systems are defined. The algebra of such systems is proposed.

Keywords: attributed transition systems without hidden transitions and their compositions, safeness and correctness, the structure of sets of states, histories and traces.

СИСТЕМНИЙ АНАЛІЗ **SYSTEMS ANALYSIS**

УДК 519.21

Динамическое слияние глобальной и локальной моделей для устойчивого планирования землепользования с учетом глобальных проекций GLOBIOM и локальных технико-экономических и ресурсных ограничений / Ермольева Т.Ю., Ю.М. Ермольев, П. Хавлик, А. Монье, Д. Леклер, С. Фритц, Х. Валин, М. Оберштайнэр, С.В. Киризюк, Е.Н. Бородина // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 16–30.

Іл.: 1. Табл. 0. Бібліогр.: 19 назв.

В целях проведения исследований и получения прогнозов на требуемом пространственном разрешении объединены две модели: вычисление глобальных и региональных проекций осуществляется с помощью глобальной динамической модели частичного равновесия GLOBIOM (Global Biosphere Management Model), а уменьшение размерности полученных результатов до необходимых пространственных разрешений проводится с помощью динамической рекурсивной модели разукрупнения, использующей принцип кросс-энтропии. Предложенный подход позволяет учесть данные, имеющиеся на разных разрешениях и из разных источников. В практических исследованиях, проведенных в Китае и Украине, предложенный подход позволил получить локальные прогнозы развития и изменения землепользования, соответствующие реальным тенденциям и ожиданиям. Разукрупненные данные и проекции использовались в национальных моделях планирования устойчивого землепользования и сельскохозяйственного развития.

Ключевые слова: глобальная модель планирования землепользования, модель робастного разукрупнения, динамическое слияние моделей, неопределенности, локальные проекции землепользования.

Динамічне злиття глобальної і локальної моделей для сталого планування землекористування з урахуванням глобальних проекцій GLOBIOM і локальних техніко-економічних ресурсних обмежень / Т.Ю. Єрмольєва, Ю.М. Єрмольєв, П. Хавлик, А. Моньє, Д. Леклер, С. Фрітц, Х. Валін, М. Оберштайнер, С.В. Киризюк, О.М. Бородіна // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 16–30.

З метою проведення досліджень і отримання прогнозів на необхідній просторовій одиниці запропоновано об'єднати дві моделі: обчислення глобальних і регіональних проекцій здійснюють за допомогою глобальної динамічної моделі часткової рівноваги GLOBIOM (Global Biosphere Management Model), а зменшення розмірності отриманих результатів до необхідної просторової одиниці отримують за допомогою динамічної рекурсивної моделі розукрупнення, що використовує принцип крос-ентропії. Запропонований підхід дозволяє врахувати наявні на різних просторових одиницях і з різних джерел дані. У практичних дослідженнях, проведених у Китаї та Україні, запропонований підхід дозволив отримати локальні прогнози розвитку і зміни землекористування, що відповідають реальним тенденціям і очікуванням. Розукрупнені дані і проекції використано в національних моделях планування сталого землекористування та сільськогосподарського розвитку.

Ключові слова: глобальна модель планування землекористування, модель робастного розукрупнення, динамічне злиття моделей, невизначеності, локальні проекції землекористування.

Dynamic linkage of global and local models for sustainable land use planning accounting for global projections from GLOBIOM and local feasibility and resource constraints / T.Y. Ermolieva, Y.M. Ermoliev, P. Havlík, A. Mosnier, D. Leclere, S. Fritz, H. Valin, M. Obersteiner, S.V. Kyryzyuk, E.N. Borodina // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 16–30.

In this paper, in order to conduct research at required spatial resolution, we propose a model fusion involving interlinked calculations of regional projections by a global dynamic model GLOBIOM (Global Biosphere Management Model) and a robust dynamic downscaling model, based on cross-enthropy principle, for deriving spatially resolved projections. The proposed procedure allows incorporating data from satellite images, statistics, expert opinions, as well as data from global land use models. In numerous case studies in China and Ukraine, the approach allowed to estimate local land use and land use change projections correspondingto real trends and expectations. The disaggregated data and projections were used in national models for planning sustainable land use and agricultural development.

Keywords: global land use model, robust downscaling, dynamic model fussion, uncertainities, local land use projections.

УДК 519.6

Методы построения точной разностной схемы для обыкновенного дифференциального уравнения четвертого порядка / Приказчиков В.Г. // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 31–37.

Іл.: 0. Табл. 0. Бібліогр.: 9 назв.

Рассматривается построение точных разностных схем для уравнения четвертого порядка с переменными коэффициентами. Для построения использованы полученные в явном виде решения задачи Коши.

Ключевые слова: точная разностная схема, задача Коши, сплайны, однородное уравнение.

Методи побудови точної різницевої схеми для звичайного диференціального рівняння четвертого порядку / В.Г. Приказчиков // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 31–37.

Розглянуто побудову точних різницевих схем для рівняння четвертого порядку зі змінними коефіцієнтами. Для побудови використано отримані в явному вигляді розв'язки задачі Коші.

Ключові слова: точна різницева схема, задача Коші, сплайни, однорідне рівняння.

Methods to construct the exact difference scheme for a differential equation of order 4 / V.G. Prikazchikov // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 31–37.

The paper deals with the construction of exact difference schemes for fourth-order equations with variable coefficients. To this end, we use the explicit solutions of the Cauchy problem.

Keywords: exact difference scheme, Cauchy problem, splines, homogeneous equation.

УДК 517.9:519.6
Об устойчивости разностных схем расщепления для уравнения конвективной диффузии / А.В. Гладкий // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 38–50.

Іл.: 0. Табл. 0. Бібліогр.: 16 назв.

Рассмотрена задача численного моделирования процессов распространения загрязнений в атмосфере на основе метода геометрического расщепления трехмерных нестационарных уравнений конвективной диффузии. Для решения полученных одномерных задач построены разностные схемы расщепления бегущего счета. Исследованы вопросы аппроксимации, монотонности и устойчивости предложенных разностных схем.

Ключевые слова: уравнение конвекции-диффузии, методы расщепления, численный метод, разностная схема, устойчивость.

Про стійкість різницевих схем розщеплення для рівняння конвективної дифузії / **А.В. Гладкий** // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 38–50.

Розглянуто задачу чисельного моделювання процесів поширення забруднень у повітряному середовищі на основі методу геометричного розщеплення тривимірних нестаціонарних рівнянь конвективної дифузії. Для розв'язання отриманих одновимірних задач побудовано різницеві схеми розщеплення у вигляді схем з явною організацією обчислень. Досліджено питання апроксимації, монотонності та стійкості запропонованих різницевих схем.

Ключові слова: рівняння конвекції-дифузії, методи розщеплення, числовий метод, різницева схема, стійкість.

Stability of difference splitting schemes for the convective-diffusion equation / A.V. Gladky // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 38–50.

We consider the problem of numerical modeling of the propagation of contamination in the air processes on the basis of geometry splitting method for three-dimensional nonstationary convection-diffusion equations. Splitting difference schemes in the form of schemes with explicit computing are proposed to solve the obtained one-dimensional problems. The approximation, monotonicity, and stability of difference schemes are investigated.

Keywords: convection-diffusion equation, splitting methods, numerical method, finite difference scheme, stability.

УДК 517.9:519.6
Математическое моделирование дробно-дифференциальной фильтрационной динамики на основе модели с производной Хильфера–Прабхакара / В.М. Булавацкий // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 51–64.

Іл.: 0. Табл. 0. Бібліогр.: 24 назв.

Построена обобщенная математическая модель для описания дробно-дифференциальной динамики процессов фильтрации в трещиновато-пористых средах, основанная на использовании понятия дробной производной Хильфера–Прабхакара. В рамках указанной модели получены замкнутые решения ряда краевых задач теории фильтрации о моделировании динамики давлений при пуске скважин в случае плоско-радиальной фильтрации, а также работе галерей в условиях плоско-параллельной фильтрации.

Ключевые слова: математическое моделирование, дробно-дифференциальная динамика фильтрационных процессов, трещиновато-пористые среды, неклассические модели, уравнение фильтрации с дробной производной Хильфера–Прабхакара, краевые задачи, замкнутые решения.

Математичне моделювання дробово-диференційної фільтраційної динаміки на основі моделі з похідною Хільфера–Прабхакара / В.М. Булавацький // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 51–64.

Побудовано узагальнену математичну модель для опису дробово-диференційної динаміки процесів фільтрації в тріщинувато-пористих середовищах, яка грунтується на використанні поняття дробової похідної Хільфера–Прабхакара. У рамках зазначеної моделі одержано замкнені розв'язки низки крайових задач теорії фільтрації щодо моделювання динаміки тисків при пуску свердловин у випадку пласкорадіальної фільтрації, а також роботі галерей за умов пласкопаралельної фільтрації.

Ключові слова: математичне моделювання, дробово-диференційна динаміка фільтраційних процесів, тріщинувато-пористі середовища, некласичні моделі, рівняння фільтрації з дробовою похідною Хільфера–Прабхакара, крайові задачі, замкнені розв'язки.

Mathematical modeling of fractional differential filtration dynamics based on models with Hilfer–Prabhakar derivative / V.M. Bulavatsky // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 51–64.

We construct a generalized mathematical model to describe the fractional differential dynamics of filtration processes in fractured porous media, based on the use of the concept of Hilfer-Prabhakar fractional derivative. Within the framework of this model, we obtain a number of closed solutions to boundary-value problems of filtration theory for modeling the dynamics of pressures at launch of wells in case of plane-radial filtration, as well as by activity of galleries under plane-parallel filtration.

Keywords: mathematical modeling, fractional-differential dynamics of filtration processes, fractured porous media, non-classical models, equation of filtration with Hilfer–Prabhakar fractional derivative, boundary value problems, closed form solutions.

УДК 519.2

Наибольшая точная нижняя граница вероятности отказа системы в специальном интервале времени при неполной информации о функции распределения времени до отказа системы / Л.С. Стойкова // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 65–73.

Іл.: 0. Табл. 2. Бібліогр.: 7 назв.

Решается задача нахождения точных нижних границ вероятности $F(v) - F(u)$, $0 < u < v < \infty$, где $u = m - \sigma_\mu 3\sqrt{3}$, $v = m + \sigma_\mu 3\sqrt{3}$, σ_μ — заданная дисперсия в множестве функций распределения $F(x)$ неотрицательных случайных величин с унимодальной дифференцируемой плотностью с модой, равной m, и двумя первыми фиксированными моментами μ_1, μ_2. Рассматривается случай, когда мода совпадает с первым моментом: $m = \mu_1$. Найдена наибольшая вероятность из всех точных нижних границ вероятностей для решаемой задачи, и она является близкой к единице, т.е. равной 0,98430.

Ключевые слова: экстремум линейного функционала, класс унимодальных функций распределения с двумя первыми фиксированными моментами, разбиение области параметров.

Найбільша точна нижня границя ймовірності відмови системи в спеціальному інтервалі часу при неповній інформації щодо функції розподілу часу до відмови системи / Л.С. Стойкова // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 65–73.

Розв'язується задача знаходження точних нижніх границь імовірності $F(v) - F(u)$, $0 < u < v < \infty$, де $u = m - \sigma_\mu 3\sqrt{3}$, $v = m + \sigma_\mu 3\sqrt{3}$, σ_μ — фіксована дисперсія в множині функцій розподілу $F(x)$ невід'ємних випадкових величин з унімодальною диференційованою щільністю з модою, рівною m, і двома першими фіксованими моментами μ_1, μ_2. Розглянуто випадок, коли мода збігається з першим моментом: $m = \mu_1$. Знайдено найбільшу ймовірність із всіх точних нижніх границь ймовірностей для даної задачі, і вона є близькою до 1, а саме рівна 0,98430.

Ключові слова: екстремум лінійного функціоналу, клас унімодальних функцій розподілу з двома першими фіксованими моментами, розбиття області параметрів.

Greatest lower bound of system failure probability in a special time interval under incomplete information about the distribution function of the time to failure of system / L.S. Stoikova // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 65–73.

The author solves the problem of finding exact lower bounds for the probability $F(v) - F(u)$, $0 < u < v < \infty$ where $u = m - \sigma_\mu 3\sqrt{3}$, $v = m + \sigma_\mu 3\sqrt{3}$, and σ_μ is a fixed dispersion in the set of distribution functions $F(x)$ of non-negative random variables with unimodal differentiable density with mode m and two first fixed moments μ_1, μ_2. The case is considered where the mode coincides with the first moment: $m = \mu_1$. The greatest lower bound of all possible exact lower bounds for this problem is obtained and it is nearly one, namely, is equal to 0.98430.

Keywords: extremum of a linear functional, the set of unimodal distribution functions with two first fixed moments, partition of the domain of parameters.

УДК 621.39:623.624+623.77

Математическая модель шумовой помехи для защиты информации от утечки по техническим каналам / С.А. Иванченко // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 74–82.

Іл.: 3. Табл. 0. Бібліогр.: 15 назв.

Обоснована математическая модель шумовой помехи, учитывающая статистическую связь отсчетов считывания, для гарантированной защиты информации от утечки по техническим каналам. Модель вносит поправки в математическое ожидание и действующее среднеквадратическое отклонение, которые смещают среднюю точку помехи и определяют ее действующую мощность.

Ключевые слова: шум, шумовая помеха, математическая модель, гарантированная защита информации, утечка информации, технические каналы утечки.

Математична модель шумової завади для захисту інформації від витоку технічними каналами / **С.О. Іванченко** // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 74–82.

Обґрунтовано математичну модель шумової завади, яка враховує статистичний зв'язок відліків зчитування, для гарантованого захисту інформації від витоку технічними каналами. Модель вносить поправки в математичне сподівання та дійове середньоквадратичне відхилення, які зміщують середню точку завади і визначають дійову потужність.

Ключові слова: шум, шумова завада, математична модель, гарантований захист інформації, витік інформації, технічні канали витоку.

Mathematical model of noise interference for information protection against leakage by technical channels / S.A. Ivanchenko // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 74–82.

The author substantiates the mathematical model of noise interference that takes into account statistical relation of readout samples for secure information protection against leakage by technical channels. The model amends the mathematical expectation and root-mean-square deviation, which shifts the midpoint of noise interference and determoines its effective capacity.

Keywords: noise, noise interference, mathematical model, secure information protection, information leakage, technical channels of leakage.

УДК 517.988

Вариант метода зеркального спуска для вариационных неравенств / В.В. Семёнов // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 83–93.

Іл.: 0. Табл. 0. Бібліогр.: 29 назви.

Метод зеркального спуска был предложен в конце 70-х годов XX в. для задач выпуклой оптимизации. Он используется для решения задач очень больших размерностей. Описан новый вариант этого метода для решения вариационных неравенств с псевдомонотонными операторами. Его можно проинтерпретировать как модификацию двухэтапного алгоритма Попова с использованием проектирования на допустимое множество в смысле расстояния Брэгмана. Доказана теорема сходимости метода.

Ключевые слова: вариационное неравенство, псевдомонотонность, расстояние Брэгмана, расстояние Кульбака–Лейблера, метод зеркального спуска, сходимость.

Варіант методу дзеркального спуску для варіаційних нерівностей / В.В. Семенов // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 83–93.

Метод дзеркального спуску буор запропоновано в кінці 70-х років XX ст. для задач опуклої оптимізації. Він використовується для розв'язання задач дуже великих розмірностей. Описано новий варіант цього методу для розв'язання варіаційних нерівностей з псевдомонотонними операторами. Його можна проінтерпретувати як модифікацію двоетапного алгоритму Попова з використанням проектування на допустиму множину у розумінні відстані Брегмана. Доведено теорему про збіжність методу.

Ключові слова: варіаційна нерівність, псевдомонотонність, відстань Брегмана, відстань Кульбака–Лейблера, метод дзеркального спуску, збіжність.

A variant of mirror descent method to solve variational inequalities / V.V. Semenov // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 83–93.

The mirror descent algorithm was proposed by Nemirovski and Yudin in the end of 1970s to solve convex optimization problems. This method is suitable to solve huge-scale optimization problems. In the paper, we describe a new version of the mirror descent method to solve variational inequalities with pseudomonotone operators. The method can be interpreted as a modification of Popov's two-step algorithm with the use of Bregman projections on the feasible set. We prove the convergence of the sequences generated by the proposed method.

Keywords: variational inequality, pseudomonotonicity, Bregman distance, Kullback–Leibler distance, mirror descent method, convergence.

УДК 519.85

Лексикографическая эквивалентность в частично комбинаторной оптимизации дробно-линейных функций на размещениях / О.А. Емец, Т.Н. Барболина // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 94–106.

Іл.: 0. Табл. 0. Бібліогр.: 14 назв.

Обоснован метод построения лексикографической эквивалентности для решения частично комбинаторных оптимизационных задач на размещениях с дробно-линейной целевой функцией и линейными дополнительными ограничениями. Метод предусматривает направленный перебор классов эквивалентности, полученных при разбиении многогранного множества на основе отношения эквивалентности. Предложены как точные, так и приближенный алгоритмы. Последний позволяет получать значение целевой функции, отличающееся от оптимума не больше, чем на заданную величину.

Ключевые слова: евклидова задача комбинаторной оптимизации, задача оптимизации на размещениях, лексикографическая эквивалентность, дробно-линейная функция.

Лексикографічна еквівалентність у частково комбінаторній оптимізації дробово-лінійних функцій на розміщеннях / О.О. Ємець, Т.М. Барболіна // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 94–106.

Обґрунтувано метод побудови лексикографічної еквівалентності для розв'язування частково комбінаторних оптимізаційних задач на розміщеннях з дробово-лінійною цільовою функцією та лінійними додатковими обмеженнями. Метод передбачає спрямований перебір класів еквівалентності, отриманих при розбитті багатогранної множини на основі відношення еквівалентності. Запропоновано як точні, так і наближений алгоритми. Останній дозволяє отримувати значення цільової функції, що відрізняється від оптимуму не більше, ніж на задану величину.

Ключові слова: евклідова задача комбінаторної оптимізації, задача оптимізації на розміщеннях, лексикографічна еквівалентність, дробово-лінійна функція.

Lexicographic equivalence in mixed combinatorial optimization of linear-fractional functions on arrangements / O.O. Iemets, T.M. Barbolina // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 1. P. 94–106.

The paper substantiates the method of constructing the lexicographic equivalence to solve mixed combinatorial optimization problems on arrangements with linear-fractional objective function and linear additional constraints. The method involves directed search of equivalence classes obtained by splitting polyhedral set using equivalence relation. The authors propose exact methods as well as an approximate one. The approximate method allows getting the objective function value that differs from the optimum by no more than a predetermined value.

Keywords: Euclidian problem of combinatorial optimization, optimization problem on arrangements, lexicographic equivalence, linear-fractional function.

УДК 621.391

Бигауссовская математическая модель сигналов источников радиоизлучений в информационной среде телекоммуникационных систем / А.А. Ильяшов // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 107–113.

Іл.: 3. Табл. 0. Бібліогр.: 6 назв.

Проанализированы причины непригодности одномерной гауссовской модели для анализа и синтеза измерений параметров сложных сигналов. Описана бигауссовская математическая модель сигналов источников радиоизлучений.

Ключевые слова: одномерная гауссовская модель сигналов источников радиоизлучений, бигауссовская математическая модель, закон Райса.

Бігаусівська математична модель сигналів джерел радіовипромінювань в інформаційному середовищі телекомунікаційних систем / О.А. Ільяшов // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 107–113.

Проаналізовано причини непридатності одновимірної ґаусівської моделі для аналізу та синтезу вимірювань параметрів складних сигналів. Описано бігаусівську математичну модель сигналів джерел радіовипромінювань.

Ключові слова: одновимірна ґаусівська математична модель сигналів джерел радіовипромінювань, бігаусівська математична модель, закон Райса.

The bi-Gaussian mathematical model of the signal sources from radio emitting in the information environment in telecommunication systems / O.A. Iliashov // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 107–113.

This paper analyzes why the one-dimensional Gaussian model is inapplicable for the analysis and synthesis of measurements of parameters of complex signals and describes the bi-Gaussian mathematical model of signals of sources of radio emitting.

Keywords: one-dimensional the Gaussian mathematical model of the signals sources radio emitting, the bi-Gaussian mathematical model, the Rice law.

УДК 621.391:519.2

Стойкие и практичные рандомизированные поточные шифры на основе кодов Рида–Соломона / А.Н. Алексейчук, С.В. Гришаков // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 114–121.

Іл.: 0. Табл. 1. Бібліогр.: 12 назв.

Рассмотрен класс рандомизированных поточных шифров, основанных на совместном применении шифрования, случайного кодирования и помехоустойчивого кодирования открытых сообщений двоичны-

ми линейными кодами. Показано, что в этом классе существуют шифры, имеющие сколь угодно высокую вычислительную стойкость относительно наиболее мощной из известных атак и обеспечивающие сколь угодно близкие к единице скорость передачи, достоверность приема, а также приемлемую сложность восстановления открытых сообщений законным получателем. Доказательство является конструктивным.

Ключевые слова: рандомизированный поточный шифр, случайное кодирование, корреляционная атака, обоснованная стойкость, код Рида–Соломона.

Стійкі та практичні рандомізовані потокові шифри на базі кодів Ріда–Соломона / А.М. Олексійчук, С.В. Гришаков // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 114–121.

Розглянуто клас рандомізованих потокових шифрів, що базуються на сумісному застосуванні шифрування, випадкового кодування та завадостійкого кодування відкритих повідомлень двійковими лінійними кодами. Показано, що в цьому класі існують шифри, що мають як завгодно високу обчислювальну стійкість відносно найбільш потужної з відомих атак та забезпечують як завгодно близькі до одиниці швидкість передачі, достовірність прийому, а також прийнятну складність відновлення відкритих повідомлень законним одержувачем. Доведення є конструктивним.

Ключові слова: рандомізований потоковий шифр, випадкове кодування, кореляційна атака, обґрунтована стійкість, код Ріда–Соломона.

Secure and practical randomized stream ciphers based on Reed–Solomon codes / A.N. Alekseychuk, S.V. Gryshakov // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 114–121.

In this paper we consider a class of randomized stream ciphers based on joint employment of encryption, random coding, and error-correction coding by binary linear codes. It is shown that in this class there exist ciphers that have arbitrarily high computational security against the most powerful from all known attacks providing that both the transmission rate and the receiving accuracy have the value arbitrarily close to 1. The complexity of recovering plain messages by the legitimate receiver is acceptable as well. The proof is constructive.

Keywords: randomized stream cipher, random coding, correlation attack, provable security, Reed-Solomon code.

УДК 519.872

Оценка стационарных вероятностей состояний системы обслуживания $\bullet / G / \infty$ при различных видах входящего потока требований / И.Н. Кузнецов, А.А. Шумская // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 122–133.

Іл.: 0. Табл. 2. Бібліогр.: 30 назв.

Рассмотрены пять моделей входящего потока существенно более сложной структуры, чем пуассоновский, когда стационарные вероятности состояний системы $\bullet / G / \infty$ находятся в явном виде (распределение Пуассона). Для представленных моделей сочетание распределения Пуассона (аналитическая часть) со статистическим моделированием (статистическая часть) позволяет находить стационарные вероятности состояний ускоренным моделированием. Точность полученных оценок проиллюстрирована численными примерами.

Ключевые слова: система обслуживания, стационарные вероятности состояний, нестационарный пуассоновский процесс, регенерирующий процесс, полумарковский процесс, процесс скоплений, несмещенная оценка, относительная погрешность.

Оцінка стаціонарних ймовірностей станів системи обслуговування $\bullet / G / \infty$ при різних видах вхідного потоку вимог / І.М. Кузнецов, А.А. Шумська // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 122–133.

Розглянуто п'ять моделей вхідного потоку істотно більш складної структури, ніж пуасонівський, коли стаціонарні ймовірності станів системи $\bullet / G / \infty$ знаходяться у явному вигляді (розподіл Пуасона). Для наведених моделей поєднання розподілу Пуасона (аналітична частина) із статистичним моделюванням (статистична чистина) дозволяє знаходити стаціонарні ймовірності станів прискореним моделюванням. Точність оцінок проілюстровано числовими прикладами.

Ключові слова: система обслуговування, стаціонарні ймовірності станів, нестаціонарний пуасонівський процес, регенерувальний процес, напівмарковський процес, процес скупчень, незміщена оцінка, відносна похибка.

The evaluation of steady-state probabilities of queueing system $\bullet / G / \infty$ for different input flow models / I.N. Kuznetsov, A.A. Shumskaya // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 122–133.

We consider five input flow models of more complicated structure than the Poisson one, where steady-state probabilities of the queueing system $\bullet / G / \infty$ can be found explicitly (the Poisson distribution). For these models, the combination of Poisson distribution (analytical part) with statistical simulation (statistical part) allows us to evaluate the steady-state probabilities with the fast simulation method. The accuracy of the estimates is illustrated by numerical examples.

Keywords: queueing system steady-state probabilities, nonstationary Poisson flow, regenerative process, semi-Markov process, cluster process, unbiased estimate, relative error.

УДК 519.21
Определение стационарных характеристик трехканальных систем с эрланговским распределением времени обслуживания / Ю.В. Жерновый, К.Ю. Жерновый // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 134–145.

Іл.: 0. Табл. 2. Бібліогр.: 11 назв.

Предложен метод исследования систем обслуживания $M/E_2/3/m$: стандартной системы, а также систем с пороговой и гистерезисной стратегиями случайного отбрасывания заявок в целях управления входящим потоком. Получены рекуррентные соотношения для вычисления стационарного распределения числа заявок в системе и стационарных характеристик. Построенные алгоритмы проверены на примерах с использованием имитационных моделей, созданных с помощью инструментальных средств GPSS World.

Ключевые слова: трехканальная система обслуживания, простейший входящий поток, эрланговское распределение времени обслуживания, случайное отбрасывание заявок, метод фиктивных фаз, рекуррентные соотношения.

Визначення стаціонарних характеристик триканальних систем з ерлангівським розподілом часу обслуговування / Ю.В. Жерновий, К.Ю. Жерновий // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 134–145.

Запропоновано метод дослідження систем обслуговування $M/E_2/3/m$: стандартної системи та систем з пороговою і гістерезисною стратегіями випадкового відкидання замовлень з метою управління вхідним потоком. Отримано рекурентні співвідношення для обчислення стаціонарного розподілу кількості замовлень у системі та стаціонарних характеристик. Побудовані алгоритми перевірено на прикладах з використанням імітаційних моделей, створених за допомогою інструментальних засобів GPSS World.

Ключові слова: триканальна система обслуговування, найпростіший вхідний потік, ерлангівський розподіл часу обслуговування, випадкове відкидання замовлень, метод фіктивних фаз, рекурентні співвідношення.

Determination of steady-state characteristics of three-channel queueing systems with Erlangian service times / Yu.V. Zhernovyi, K.Yu. Zhernovyi // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 134–145.

We propose a method to analyze $M/E_2/3/m$ queueing systems: standard system and systems with the threshold and hysteretic strategies of random dropping of customers in order to control the input flow. We obtain recurrence relations to compute the stationary distribution of the number of customers and the steady-state characteristics. The developed algorithms are tested on the examples using simulation models constructed with the assistance of the GPSS World tools.

Keywords: three-channel queueing system, Poisson input, Erlangian service times, random dropping of customers, fictitious phase method, recurrence relations.

УДК 330.101.541-336.7
Динамика экономических циклов / Б.Б. Дунаев // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 146–162.

Іл.: 2. Табл. 4. Бібліогр.: 35 назви.

Определено циклическое во времени развитие экономики как результат имевшихся и имеющихся изменений соотношения спроса и предложения на рынке благ, нарушивших равновесие, которое восстанавливается с постоянными временными ритмами в процессе саморегулирования рыночной системой количества работающих в сфере производства по конъюнктуре потребительского спроса. Показано, что наблюдаемые волны Кондратьева измеряются в базовых ценах реальной стоимостью имеющегося в сфере производства капитала и представляются ее графиками во времени.

Ключевые слова: экономика, рынок, циклы, спрос, предложение, равновесие, кризис, конъюнктура, труд, капитал, деньги, воспроизводство, инвестиции, инфляция.

Динаміка економічних циклів / Б.Б. Дунаєв // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 146–162.

Визначено циклічний за часом розвиток економіки як результат тих, що були, і наявних змін співвідношення попиту і пропозиції на ринку благ, які порушили рівновагу, що відновлюється з постійними тимчасовими ритмами в процесі саморегулювання ринковою системою кількості працівників у сфері виробництва за кон'юнктурою споживчого попиту. Показано, що спостережувані хвилі Кондратьєва вимірюються в базових цінах реальною вартістю наявного в сфері виробництва капіталу і є її графіками у часі.

Ключові слова: економіка, ринок, цикли, попит, пропозиція, рівновага, криза, кон'юнктура, праця, капітал, гроші, відтворення, інвестиції, інфляція.

Dynamics of economic cycles / B.B. Dunaev // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 146–162.

Cyclic economic development results from the available and current changes in the balance between supply and demand in the goods market that disturb the equilibrium, which is recovering at time constant rhythms during self-regulation by the market system of the number of employees in production on market conditions in consumer demand. It is shown that the observed Kondratieff waves measured in the real value of the existing capital and production are its time schedules.

Keywords: economy, market, cycles, demand, supply, equilibrium, crisis, environment, labor, capital, money, reproduction, investments, inflation.

УДК 519.854

Повторяемый итерированный алгоритм табу для решения квадратичной задачи о назначениях / П.В. Шило // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 163–167.

Іл.: 0. Табл. 1. Бібліогр.: 18 назв.

Разработан новый алгоритм повторяемого табу для решения квадратичной задачи о назначениях. Проведенное сравнительное исследование данного алгоритма с лучшими в настоящее время алгоритмами решения этой задачи показало его конкурентоспособность как по быстродействию, так и по возможности получения лучших решений.

Ключевые слова: квадратичная задача о назначениях, табу, вычислительный эксперимент, сравнительное исследование алгоритмов.

Повторюваний ітерований алгоритм табу для розв'язання квадратичної задачі про призначення / П.В. Шило// Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 163–167.

Розроблено новий алгоритм повторюваного табу для розв'язання квадратичної задачі про призначення. Проведене порівняльне дослідження цього алгоритму з найкращими на даний час алгоритмами розв'язання цієї задачі показало його конкурентоспроможність як за швидкодією, так і за можливістю отримання кращих розв'язків.

Ключові слова: квадратична задача про призначення, табу, обчислювальний експеримент, порівняльне дослідження алгоритмів.

Solving the quadratic assignment problem by the repeated iterated tabu search method / P.V. Shylo // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 163–167.

A novel Repeated Iterated Tabu Search for quadratic assignment problem is presented. We compare our approach to the state-of-the-art techniques and demonstrate its advantages with respect to run times and solution quality.

Keywords: quadratic assignment problem, tabu search, computing experiment, a comparative study of algorithms.

ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ — SOFTWARE–HARDWARE COMPLEXES

УДК 004.04

Управление ресурсами распределенной компьютерной системы с учетом уровня доверия к вычислительным компонентам / Чженбин Ху, В.Е. Мухин, Я.И. Корнага, О.Ю. Герасименко // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 168–180.

Іл.: 3. Табл. 2. Бібліогр.: 31 назва.

Рассматривается обеспечение безопасной обработки данных в распределенных компьютерных системах (РКС), что является важным для выполнения определенного класса задач. Предложен подход к управлению ресурсами РКС, который в соответствии с требованиями пользователя позволяет учесть как временные затраты на выполнение задания, так и уровень защищенности ресурсов, привлекаемых для его выполнения.

Ключевые слова: распределенные вычисления, управление ресурсами, планирование задач, безопасная обработка данных, мониторинг состояния вычислительного узла, локальный агент данных.

Управління ресурсами розподіленої комп'ютерної системи з урахуванням рівня довіри до обчислювальних компонентів / Чженбін Ху, В.Є. Мухін, Я.І. Корнага, О.Ю. Герасименко // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 168–180.

Розглянуто гарантування безпечного оброблення даних у розподілених комп'ютерних системах (РКС), що є критично важливим для виконання певного класу задач. Запропоновано підхід до управління ресурсами РКС, який відповідно до вимог користувача дозволяє врахувати як витрати часу на виконання завдання, так і рівень захищеності ресурсів, які залучаються для його виконання.

Ключові слова: розподілені обчислення, управління ресурсами, планування завдань, безпечне оброблення даних, моніторинг стану обчислювального вузла, локальний агент даних.

Resource management in distributed computer system taking into account the trust level to the computational nodes / **Zhengbing Hu, V.Ye. Mukhin, Ya.I. Kornaga, O.Yu. Herasymenko** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 168–180.

The safe data processing in distributed computer system (DCS) is critical for a certain class of computational tasks. This paper describes an approach to resource management in DCS, which, according to user's requirements, allows taking into account the task execution time as well as the security level of system's resources.

Keywords: distributed computing, resource management, scheduling, secure data processing, computing node state monitoring, local data agent.

УДК 681.3

Онтологические и алгеброалгоритмические средства автоматизации проектирования параллельных программ для «облачных» платформ / А.Е. Дорошенко, О.М. Овдей, Е.А. Яценко // Кибернетика и системный анализ. 2017. Том 53, № 2. С. 181–192.

Іл.: 2. Табл. 5. Бібліогр.: 20 назви.

Предложен подход к автоматизированной разработке программ, основанный на использовании средств онтологий и алгеброалгоритмического инструментария проектирования и синтеза программ. Применение подхода проиллюстрировано на примере разработки параллельной программы из области метеорологического прогнозирования, а также приложения, предназначенного для выполнения созданной программы в «облачной» среде.

Ключевые слова: онтология, алгебра алгоритмов, проектирование и синтез программ, параллельная программа, «облачные» вычисления.

Онтологічні та алгеброалгоритмічні засоби автоматизації проектування паралельних програм для «хмарних» платформ / А.Ю. Дорошенко, О.М. Овдій, О.А. Яценко // Кібернетика та системний аналіз. 2017. Том 53, № 2. С. 181–192.

Запропоновано підхід до автоматизованого розроблення програм, що ґрунтується на використанні засобів онтологій та алгеброалгоритмічного інструментарію проектування і синтезу програм. Застосування підходу проілюстровано на прикладі розроблення паралельної програми у сфері метеорологічного прогнозування, а також програмного застосунку, призначеного для виконання створеної програми в «хмарному» середовищі.

Ключові слова: онтологія, алгебра алгоритмів, проектування і синтез програм, паралельна програма, «хмарні» обчислення.

Ontological and algebra-algorithmic tools for automated design of parallel programs for cloud platforms / **A.Yu. Doroshenko, O.M. Ovdii, O.A. Yatsenko** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 2. P. 181–192.

We propose an approach to automated development of programs, which is based on the use of ontological facilities and algebra-algorithmic tools for design and synthesis of programs. The approach is illustrated on the example of developing a parallel program in the meteorological forecasting domain, as well as software application to execute the developed program on a cloud computing platform.

Keywords: ontology, algebra of algorithms, design and synthesis of programs, parallel program, cloud computing.