КІБЕРНЕТИКА **CYBERNETICS**

УДК 519.872

Огляд моїх наукових робіт. Учителі та соратники / Коваленко І.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 3–27.

Автор робить огляд своїх публікацій, віддаючи належне видатним математикам, своїм науковим керівникам Б.В. Гнеденку, О.М. Колмогорову, В.С. Михалевичу, В.С. Королюку та іншим. Бібліогр.: 169 назв.

UDC 519.872

A survey of my scientific publications. Masters and co-workers / Kovalenko I.N. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 3–27.

The author surveys his publications doing justice to famous mathematicians B.V. Gnedenko, A.N. Kolmogorov, V.S. Mikhalevich, V.S. Koroliuk, and some others, who superwised him. Refs: 169 titles.

УДК 519.21

Розв'язання проблеми інваріантності ймовірнісних характеристик заздалегідь сумісних систем випадкових нелінійних рівнянь над скінченним комутативним кільцем з одиницею / Левітська А.О. // Кибернетика и системный анализ. — 2010. — № 3. — С. 28–41.

Розглянуто один клас заздалегідь сумісних систем випадкових нелінійних рівнянь над довільним скінченним комутативним кільцем з одиницею. Досліджуються питання про межу області інваріантності і відповідно граничних факторіальних моментів числа ненульових розв'язків, відмінних від фіксованого розв'язку даної системи, та граничного розподілу числа таких розв'язків, а також вивчається їх геометрична структура, коли число невідомих в системі прямує до нескінченності. Бібліогр.: 10 назв.

UDC 519.21

Solving a problem of invariance of probability characteristics of a priory solvable system of random non-linear equations over a finite commutative ring with an unit / Levitskaja A.A. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 28–41.

A class of a priory solvable system of random non-linear equations over a finite commutative ring with an unit is considered. The problems on the bounds of the invariance domains for the limit factorial moments and the limit distribution of the number of solutions which are different from fixed solution of the system respectively, and the geometrical structure of this solutions are investigated. Refs: 10 titles.

УДК 621.391:519.2

Верхні оцінки незбалансованості білінійних апроксимацій раундових функцій блокових шифрів / Олексійчук А.М., Шевцов А.С. // Кибернетика и системный анализ. — 2010. — № 3. — С. 42–51.

Досліджуються властивості раундових функцій блокових шифрів, що характеризують їх практичну стійкість відносно білінійного методу криптоаналізу. Отримано верхні межі незбалансованості білінійних апроксимацій раундових функцій шифрів, які містять ключовий суматор за модулем степеня числа 2, зокрема алгоритмів шифрування ГОСТ та «Калина». Бібліогр.: 13 назв.

UDC 621.391:519.2

Upper estimates of imbalance of bilinear approximations for raund functions of block ciphers / Alekseychuk A.N., Schevtsov A.S. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 42–51.

The raund functions properties of block ciphers that characterize practical security against bilinear cryptanalysis techniques are researched. Upper bounds of imbalance of bilinear approximations for raund functions of block ciphers with key adder modulo the degree of number 2, in particular, the encryption algorithms of the GOST and "Kalina" are obtained. Refs: 13 titles.

УДК 681.3.06:519.248.681

Про роботи київської школи теоретичної криптографії / Савчук М.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 52–68.

Наведено огляд робіт фахівців київської школи теоретичної криптографії переважно за останні два десятиліття в областях криптографічних методів захисту інформації, криптоаналізу і пов'язаними з ними математичними проблемами. Наведено список доповідей, заслуханих і обговорених на київському науковому семінарі «Проблеми сучасної криптології» за 2001–2009 рр. Бібліогр.: 77 назв.

UDC 681.3.06:519.248.681

On the work of the Kiev school of theoretical cryptography / Savchuk M.N. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 52–68.

We review the work of specialists of the Kiev school of theoretical cryptography mainly the last two decades in the areas of cryptographic methods of information security, cryptanalysis, and related mathematical problems. Refs: 77 titles.

УДК 519.12

Застосування прискореного моделювання для оцінки кількості деяких *k*-вимірних підпросторів над скінченним полем / Масол В.І., Кузнєцов І.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 69–83.

Запропоновано метод прискореного моделювання для обчислення кількості k-вимірних підпросторів ваги ω n-вимірного векторного простору над полем Галуа, що містить q елементів. Для $\omega = 1$ та $\omega = 2$ будуються незміщені оцінки, а для $\omega = 3$ — верхні та нижні оцінки. Доведено обмеженість відносної середньоквадратичної похибки оцінок при $q \to \infty$. Високу точність методу ілюструють чисельні приклади. Табл.: 2. Бібліогр.: 9 назв.

UDC 519.12

Application of the fast simulation method to the evaluation of the number of some *k*-measurable subspaces over a finite space / Masol V.I., Kuznetsov I.N. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 69–83.

A fast simulation method for the evaluation of the number of k-measurable subspaces of the weight ω of n-measurable vector+ space over the Galois field containing q components is proposed. The unbiased estimates are constructed for the cases $\omega = 1$ and $\omega = 2$, and lower and upper estimates are proposed for the case $\omega = 3$. It is proved that relative error remains bounded as $q \to \infty$. High accuracy of the method proposed is demonstrated on numerical examples. Tabl.: 2. Refs: 9 titles.

СИСТЕМНИЙ АНАЛІЗ **SYSTEMS ANALYSIS**

УДК 519.872

До класифікації систем масового обслуговування з повторенням викликів / Коваленко І.М., Коба О.В. // Кибернетика и системный анализ. — 2010. — № 3. — С. 84–91.

Вводяться типові класи систем обслуговування з повторенням викликів, що виникають з практичних задач. Дано коротку порівняльну характеристику систем з повторенням різних класів. Запропоновано їх кодування. Іл.: 7. Бібліогр.: 14 назв.

UDC 519. 872

On the classification of retrial queueing systems / Kovalenko I.N., Koba E.V. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 84–91.

The authors introduce some typical classes of retrial queueing systems which are taken from applied problems. Some indexes of different types of such systems are compared numerically. Coding of retrial queueing is discussed as well. Figs: 7. Refs: 14 titles.

УДК 519.872

Деякі результати для системи обслуговування *GI* / *G* / *n* / 0 з використанням евристики *GM* / Аткінсон Дж.Б., Коваленко І.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 92–100.

Проаналізовано ймовірность втрати вимоги в багатоканальній системі обслуговування з відмовами *GI* / *G* / *n* / 0 як у випадку малого навантаження, так і великого. Аналіз оснований на евристиці *GM* , для якої випадок помірного навантаження детально вивчено раніше. Знайдено достатні умови для асимптотичної точності евристики *GM* у випадку малого навантаження. Ця евристика має вказану властивість також у випадку великого навантаження, якщо число каналів *n* прямує до нескінченності. Іл.: 4. Бібліогр.: 8 назв.

UDC 519.872

Some light-traffic and heavy-traffic results for the *GI* / *G* / *n* / 0 queue using the *GM Heuristic* / Atkinson J.B., Kovalenko I.N. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 92–100.

In this paper we carry out both light-traffic and heavy-traffic analyses for the calculation of steady-state loss probabilities in the general multi-server queueing loss system, the *GI* / *G* / *n* / 0 queue. The analysis makes use of a heuristic approach called the *GM Heuristic*, for which a detailed analysis in normal traffic has previously been published. Sufficient conditions are given for the *GM Heuristic* to be asymptotically exact in light traffic. The heuristic is also shown to be asymptotically exact in heavy-traffic when the number of servers *n* tends to infinity. These results are illustrated numerically using two-phase Coxian distributions for both the inter-arrival time and service time. Figs: 4. Refs: 8 titles.

УДК 519.21

Про деякі напрямки досліджень, ініційовані роботами академіка І.М. Коваленка / Кузнєцов М.Ю. // Кибернетика и системный анализ. — 2010. — № 3. — С. 101–108.

Наведено огляд деяких напрямків досліджень, які були ініційовані І.М. Коваленком та знайшли відображення у сумісних роботах з автором даної статті. До них відносяться: метод «штучних» моментів регенерації, асимптотична нечутливість, метод Монте-Карло та методи зменшення дисперсії оцінок, принцип монотонних відмов. Бібліогр.: 31 назва.

UDC 519.21

On some research guidelines initiated by articles of Academician I.N. Kovalenko / Kuznetsov N.Yu. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 101–108.

A review of some research guidelines which were initiated by I.N. Kovalenko and used in joint articles with the author is given. These are: method of «artificial» regeneration moments, asymptotic insensitivity, Monte Carlo method and variance reduction methods, principle of monotone failures. Refs: 31 titles.

УДК 619.248

Оцінювання параметрів надійності в умовах недостатньої інформації / Голодніков О.М., Єрмольєв Ю.М., Кнопов П.С. // Кибернетика и системный анализ. — 2010. — № 3. — С. 109–125.

Запропоновано алгоритм пошуку нижньої границі байєсівської оцінки параметру експоненціального розподілу за умов, коли відомо, що апріорний розподіл належить класу, який складається із всіх функцій розподілу, що мають однакові два квантилі. Ця задача виникає при аналізі чутливості байєсівських оцінок інтенсивностей відмов до вибору апріорного розподілу в експоненціальній моделі відмов. Бібліогр.: 29 назв.

UDC 619.248

Estimation of reliability parameters under insufficient information / Golodnikov A.N., Ermoliev Yu.M., Knopov P.S. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 109–125.

The paper presents algorithms of seeking lower bound of Bayesian estimates of parameter of exponential distribution in case when it is known that prior distribution belongs to class of all distribution functions with fixed two quantiles. This problem arises in sensivity analysis of Bayesian estimates of failure rates to choice prior distribution in the exponential model of failure. Refs: 29 titles.

УДК 519.872

Наближений розрахунок моделей бездротових мереж мікростільникової структури із чергами різнотипних викликів / Пономаренко Л.А., Меліков А.З., Фаттахова М.І. // Кибернетика и системный анализ. — 2010. — № 3. — С. 126–138.

Розроблено алгоритми наближених обчислень характеристик мікростільникових бездротових мереж із чергами нових і хендовер-викликів. Передбачається, що різні види викликів можуть покинути чергу, якщо час їх очікування перевищує деяке порогове значення. Наводяться результати числових експериментів. Іл.: 7. Табл.: 2. Бібліогр.: 16 назв.

UDC 519.872

Approximate calculation of the models of microcellular wireless networks with queues of heteregenous calls / Ponomarenko L.A., Melikov A.Z., Fattakhova M.I. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 126–138.

Algorithms for approximate calculation of characteristics of micro-cellular wireless networks with queues of new and handover calls are developed. It is assumed that various kinds of calls might be left the queue if their waiting time is more than some threshold values. Results of numerical experiments are shown. Figs: 7. Tabl.: 2. Refs: 16 titles.

УДК 519.2

Узагальнені нерівності Чебишова та їх застосування в математичній теорії надійності / Стойкова Л.С. // Кибернетика и системный анализ. — 2010. — № 3. — С. 139–143.

Розглянуто задачу, результатом розв'язання якої є узагальнені нерівності Чебишова. Наведено приклади з математичної теорії надійності. Міститься короткий огляд загальних результатів і результатів, отриманих автором. Сформульовано нову проблему для подальших досліджень у даному напрямку. Іл.: 1. Бібліогр.: 18 назв.

UDC 519.2

Generalized Chebyshof inequalities and their application in mathematical reliability theory / Stoikova L.S. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 139–143.

The problem is considered which resulting solution is generalized Chebyshov inequality. Examples of the mathematical theory of reliability are given. A brief review of general results and results from the author is included. Some new problem for further research in this direction is formulated. Fig.: 1. Refs: 18 titles.

УДК 519.872

Системи з циклічним очікуванням / Лакатош Л. // Кибернетика и системный анализ. — 2010. — № 3. — С. 144–151.

Вивчається система масового обслуговування, в якій вимоги, що надходять, приймаються на обслуговування або в моменти їх надходження (якщо прилад обслуговування вільний), або в моменти, що відрізняються від них інтервалами, кратними циклу *T*. Виводяться формули для кількості вимог в системі і для часу очікування, визначено умову існування ергодичного розподілу. Бібліогр.: 15 назв.

UDC 519.872

Cyclic-waiting systems / Lakatos L. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 144–151.

One considers a queueing system where entering customers are taken for service at the moment of arrival (in case of free system) or at moments differing from it by the multiples of a cycle time *T*. One finds the generating functions of customers in the system and that of the waiting time, the stability condition is obtained. Refs: 15 titles.

УДК 519.21

Функціональна гранична теорема для гіллястих процесів з імміграцією / Лебєдєв Є.О., Семенов В.В. // Кибернетика и системный анализ. — 2010. — № 3. — С. 152–161.

Розглядається особливий випадок гіллястих процесів з імміграцією частинок у випадкові моменти часу. Параметри процесу близькі до критичних. Доведено, що певним чином нормована послідовність таких процесів збігається у рівномірній топології до дифузійного процессу. Як наслідок вивчена гранична поведінка функціоналів інтегрального типу. Бібліогр.: 6 назв.

UDC 519.21

A functional limit theorem for branching processes with immigration / Lebedev E.A., Semenov V.V. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 152–161.

A special case of branching processes with immigrants in random moments of time is considered. The process parameters are closed to critical ones. It is proved that sequence of such processes normalized by the suitable way converges weakly to a diffusion process in the uniform topology. As a consequence the limit behavior of integral functionals is studied. Refs: 6 titles.

УДК 519.872

Дослідження call-центрів як систем масового обслуговування з повторними викликами / Пустова С.В. // Кибернетика и системный анализ. — 2010. — № 3. — С. 162–168.

Розглянуто математичні моделі call-центрів, які враховують повторні виклики, а також специфіку і основні аспекти складання моделей call-центрів як систем з повторними викликами. Розглянуто системи масового обслуговування типу $M/M/c/0/L/H_j$, $M/M/c/0///E_2$, $M/M/c/0/L//E_2$ як моделей call-центрів. Наведено чисельні результати для показників функціонування цих систем. Іл. 4. Табл.: 1. Бібліогр.: 6 назв.

UDC 519.872

Investigation of call centers as retrial queueing systems / Pustova S.V. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 162–168.

The mathematical models of call centers are considered in the article taking into account retrial calls. Author considers the specificity and main aspects of construction the models of call centers as retrial queues. Queueing systems $M/M/c/0/L/H_j$, $M/M/c/0///E_2$, $M/M/c/0/L//E_2$ are considered as call centers' models. The obtained numerical results for these systems' characteristics are given. Figs: 4. Tabl.: 1. Refs: 6 titles.

УДК 519.21

Про деякі підходи до оцінювання фінансового ризику / Вовк Л.Б., Кнопов О.П., Пепеляєва Т.В. // Кибернетика и системный анализ. — 2010. — № 3. — С. 169–174.

Розглянуто задачу керування кредитними ризиками, пов'язаними з діяльністю страхових інвестиційних компаній. Запропоновано підхід з використанням оцінки CVaR, в основі якого лежать методи регресійного аналізу. Бібліогр.: 11 назв.

UDC 519.21

About some approach to the financial risk estimation / Vovk L.B., Knopov A.P., Pepeljaeva T.V. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 169–174.

The credit risk control problem for insurance investment companies activities is considered. The approach on the methods of regression analysis base with using CVaR estimation is proposed. Refs: 11 titles.

УДК 519.872

Оцінка ймовірності перетину заявок складної структури в системах обслуговування / Коба О.В., Дишлюк О.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 175–180.

Отримано оцінки для спрощення розрахунків, пов'язаних з перетином випадкових заявок, що складаються з декількох часових інтервалів. Використано аналітичні прийоми та статистичне моделювання. Результати можуть використовуватися при проектуванні комунікаційних систем. Іл.: 2. Бібліогр.: 4 назви.

UDC 519.872

Estimates for probabilities and means related to intersections of complex random calls in queueing systems / Koba E.V., Dyshliuk O.N. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 175–180.

Estimates are derived towards simplification of accounts related to intersecting random calls consisting of several time intervals. Analytical approach as well as Monte Carlo simulation is applied. The results can be applied while communication systems design. Figs: 2. Refs: 4 titles.

СТИСЛІ ПОВІДОМЛЕННЯ — BRIEF COMMUNICATIONS

УДК 681.3

Стандартизація у сфері менеджменту інформаційної безпеки / Фаль О.М. // Кибернетика и системный анализ. — 2010. — № 3. — С. 181–184.

Описано сучасний стан стандартизації в сфері менеджменту інформаційної безпеки. Розглянуто вимоги до стандартів, що розробляються, типи стандартів, принципи, яких слід дотримуватись під час розроблення стандартів. Робота грунтується на матеріалах, прийнятих в підкомітеті ПК 27 «Методи захисту» об'єднаного технічного комітету ІСО/ МЕК ОТК 1 «Інформаційні технології». Бібліогр.: 2 назви.

UDC 681.3

Standardization in information security area / Fal' A.M. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 181–184.

The article describes state of the art of the standardization in information security area. The requirements to the standards being developed, the types of standards, the principles to which it is required to follow are discussed. The contents of the article is based on the documents adopted within subcommittee 27 "Security techniques" of the joint technical committee ISO/IEC JTC 1 "Information technology". Refs: 2 titles.

УДК 519.2

Уточнення асимптотичної апроксимації розміру групи в парадоксі днів народжень / Єндовицький П.О. // Кибернетика и системный анализ. — 2010. — № 3. — С. 185–188.

Доведено дві теореми про асимптотичну поведінку розміру групи у парадоксі днів народжень. В теоремі 1 наведено асимптотично непокращувальні оцінки для розміру групи у випадку рівноймовірного та незалежного розміщення частинок по чарунках. В теоремі 2 наведено асипмптотично непокращувальні оцінки для розміру групи у випадку рівноймовірного та незалежного розміщення двох однакових комплектів частинок по чарунках. Отримані результати можна застосувати у криптографії для оцінювання трудомісткості побудови колізій хеш-функцій. Бібліогр.: 6 назв.

UDC 519.2

Asymptotic approximation of the group size in birthday paradox / Endovitskij P.A. // Kibernetika i sistemny analiz. — 2010. — N 3. — P. 185–188.

Proved two theorems about asymptotic behavior group size in birthday paradox. Theorem 1 gives asymptotically best possible estimates for group size in case uniform and independent particle occupancy in cells. Theorem 2 gives asymptotically best possible estimates for group size in case uniform and independent occupancy of two equal sets of particles in cells. These results one may apply in cryptography for estimation working time for construction collisions of hash-functions. Refs: 6 titles.