РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ
BLOCK AND SYMMETRIC CYPHERS

УДК 621. 3.06

О роли схем разворачивания ключей в атаках на итеративные шифры / *В.И. Долгов, А.А. Настенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 7 – 15.

Показано, что как и для других известных шифров показатели стойкости шифра DES к атакам линейного и дифференциального криптоанализа от схем разворачивания ключей практически не зависят. При любых схемах разворачивания ключей шифр DES после 16 циклов приходит к показателям случайной подстановки соответствующей степени. Отмечается, что утверждение о том, что для любых ключевых графиков и большинства шифров, отнесенных к марковским, распределения вероятностей дифференциалов и линейных оболочек сходятся к равномерному распределению после некоторого количества циклов, является неверным.

Табл. 4. Библиогр.: 18 назв.

УДК 621. 3.06

Про роль схем розгортання ключів у атаках на ітеративні шифри / *В.И. Долгов, А.А. Настенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 7 – 15.

Показано, що як і для інших відомих шифрів показники стійкості шифру DES до атак лінійного та диференційного криптоаналізу від схем розгортання ключів практично не залежать. При будь-яких схемах розгортання ключів шифр DES після 16 циклів приходить до показника випадкової підстановки відповідного ступеня. Відмічається, що твердження про те, що для будь-яких ключових графіків і більшості шифрів, віднесених до марківських, розподілення ймовірностей диференціалів і лінійних оболонок сходиться до рівномірного розподілу нию після деякої кількості циклів, є невірним.

Таб. 4. Бібліогр. :18 назв.

UDC 621. 3.06

On the role of key schedules in attacks on iterated ciphers / *V.I. Dolgov, A.A. Nastenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 7 – 15.

It is shown that the indices of DES cipher strength to attacks of the linear and differential cryptanalysis of the key deployment schemes are practically independent as it is for other indicators of well-known ciphers. In all schemes of keys unfolding the DES cipher after 16 cycles comes to the refractive random permutation corresponding degree. It is noted that the assertion that for any key diagrams and most of codes assigned to Markov, the distribution of differentials probability and linear hulls converges to the uniform distribution of the NIJ, after a certain number of cycles, is incorrect.

Tab. 4. Ref.: 18 items.

УДК 621. 3.06

S-блоки для современных шифров / *В. И. Долгов, Е.Д. Мельничук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 16 – 23.

Приводятся результаты оценки эффективности S-блоковых конструкций, применяемых в современных блочных симметричных шифрах. Используется новый показатель оценки эффективности S-блоковых конструкций, который строится на основе оценки числа циклов шифра, необходимых ему для прихода к стационарному состоянию, свойственному случайной подстановке. Показывается, что с высокой вероятностью случайно выбранные S-блоки по этому показателю эффективности будут обладать криптографическими свойствами, не уступающими лучшим известным конструкциям. Предлагаются конструкции случайных S-блоков для шифра Rijndael и шифров, представленных на прошедший украинский конкурс по выбору национального стандарта шифрования

Табл. 13. Библиогр.: 7 назв.

УДК 621. 3.06

S-блоки для сучасних шифрів / *В.І. Долгов, Е.Д. Мельничук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 16 – 23.

Наводяться результати оцінки ефективності S-блокових конструкцій, що застосовуються в сучасних шифрах. Використовується новий показник оцінки ефективності S-блокових конструкцій, який будується на основі оцінки числа циклів шифру, необхідних йому для приходу до стаціонарного стану, властивому випадкової підстановці. Показується, що з високою ймовірністю випадково вибрані S-блоки за цим показником ефективності будуть володіти криптографічними властивостями, що не

поступаються кращим відомим конструкціям S-блоків. Пропонуються конструкції випадкових S-блоків для шифру Rijndael і шифрів, представлених на минулий український конкурс з вибору національного стандарту шифрування.

Таб. 13. Бібліогр. : 7 назв.

UDC 621. 3.06

S-blocks for modern ciphers / *V.I. Dolgov, E.D. Melnichuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 16 – 23.

The results of evaluating the effectiveness of S-block structures used in modern ciphers variables. Use a new indicator assessing the effectiveness of S-block constructions, which is based on estimating the number of cycles of the cipher, it needs to come to steady state, characteristic of a random permutation. It is shown that with high probability of randomly selected S-boxes on the effectiveness of this indicator will have cryptographic properties, to the best-known designs S-boxes. Proposed construction of random S-boxes for the cipher Rijndael cipher, and, pre-represented in the previous Ukrainian national competition to select an encryption standard.

Tab. 13. Ref.: 7 items.

УДК 621.3.06

Криптоанализ шифра Mickey на основе анализа внутренних состояний / *А.В. Казимиров, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 24 – 30.

Рассмотрены генераторы гаммы с двумя внутренними регистрами, обновляемыми линейно и нелинейно, причем при тактировании состояния регистров являются взаимозависимыми (реализуется в виде взаимного управления). Рассматривается модель атаки, основанная на обратном тактировании генератора и анализа полученного дерева обратных состояний. Этот подход применяется к поточному шифру Mickey, полученные результаты сравниваются с известными теоретическими.

Табл. 7 Ил. 3. Библиогр.: 10 назв.

УДК 621.3.06

Криптоаналіз шифру Mickey на основі аналізу внутрішніх станів / *О.В. Казимиров, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 24 – 30.

Розглянуто генератори гами з двома внутрішніми регістрами, які оновлюються лінійно і нелінійно, причому при тактуванні стани регістрів є взаємозалежними (реалізується у вигляді взаємного управління). Розглядається модель атаки, заснована на зворотному тактуванні генератора і аналізі отриманого дерева зворотних станів. Цей підхід застосовується до потокового шифру Mickey, отримані результати порівнюються з відомими теоретичними.

Табл. 7. Іл. 3. Бібліогр.: 10 назв.

UDC 621.3.06

Mickey cipher cryptanalysis based on internal states analysis / *O.V. Kazymyrov, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 24 – 30.

The key-stream generator with the internal state split into two parts, which are updated respectively linearly and nonlinearly is considered. Moreover, the state update function also depends on the internal state of the partner register implementing the so called self-mutual control. The attack scenario based on the reverse clocking of the generator and analysis of the obtained state backward tree is proposed. This approach with Mickey stream cipher is illustrated in practice. Own practical results are compared with the previous theoretical ones.

7 tab. 3 fig. Ref.: 10 items

УДК 621. 3.06

Вырожденные подстановки / *И.В. Лисицкая* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 31 – 38.

Исследуются дифференциальные и линейные свойства подстановок, названных вырожденными, под которыми понимаются подстановки, использование которых либо не позволяет в пределах ограниченного числа циклов, однозначно определенного для каждого шифра, достичь показателей случайной подстановки, либо стационарное значение, к которому приходит шифр, не соответствует ожидаемому, свойственному случайной подстановке. Приводится оценка вероятности случайного выбора подстановки вырожденного типа. Делается вывод, что попасть на вырожденную подстановку при случайном выборе является маловероятным событием. Этим подтверждается положение, являющееся основой предложенной новой методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, состоящее в том, что все шифры после не-

большого начального числа циклов шифрования независимо от используемых S-блоков приобретают свойства случайных подстановок соответствующих степеней.

Табл. 7. Библиогр.: 12 назв.

УДК 621. 3.06

Вироджені підстановки / *І.В. Лисицька* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 31 – 38.

Досліджуються диференціальні й лінійні властивості підстановки названих виродженими, під якими розуміються підстановки, використання яких або не дозволяє в межах обмеженого числа циклів, однозначно визначеного для кожного шифру, досягти показників випадкової підстановки, або стаціонарне значення, до якого приходить шифр, не відповідає очікуваному, властивому випадкової підстановці. Наводиться оцінка ймовірності випадкового вибору підстановки виродженого типу. Робиться висновок, що потрапити на вироджения підстановку при випадковому виборі є дуже малоймовірним подією. Цим підтверджується положення, що є основою запропонованої нової методології оцінки стійкості блокових симетричних шифрів до атак диференціального та лінійного криптоаналізу, яке у тому, що всі шифри після невеликого початкового числа циклів шифрування незалежно від використовуваних S-блоків набувають властивостей випадкових підстановок відповідних степенів.

Таб. 7. Бібліогр. :12 назв.

UDC 621.3.06

Degenerated substitutions / *I.V. Lisitskaya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 31 – 38.

The differential and linear properties of these degenerate substitutions, which are defined as the substitution are studied, their use either do not allow to achieve a random permutation in a limited number of cycles, which is uniquely defined for each cipher parameters, or steady-state value, which comes to code does not match the expected inherent a random permutation. The probability of a random choice of the substitution of degenerated type is estimated. It is concluded that to get to a degenerate substitution with a random choice is a very unlikely event. This confirms the position which is the basis for the proposed new methodology for assessing the strength of block symmetric ciphers to attacks of differential and linear cryptanalysis, which consists in the fact that all ciphers after a small initial number of cycles of encryption regardless of the S-boxes acquire the properties of random permutations of the powers.

Tab.7.Ref.:12 items.

УДК 681.3.06: 519.248.681

Про доказательство отсутствия эффективных байтовых дифференциальных характеристик для Rijndael-подобных шифров / *В.И. Руженцев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 39 – 42.

Внимание сосредотачивается на уточнении представленных в одной из предыдущих работ леммы и теоремы об эффективных байтовых дифференциальных характеристиках, которые могут быть использованы в атаке усеченных дифференциалов. Представлены более корректная формулировка леммы о граничном числе активных колонок и новое доказательство теоремы об отсутствии эффективных байтовых дифференциальных характеристиках в Rijndael-подобных шифрах. Выполняется сравнение теоретически полученных оценок с полученными на практике результатами.

Табл. 1. Библиогр.: 10 назв.

УДК 681.3.06: 519.248.681

Про доведення відсутності ефективних байтових диференційних характеристик для Rijndael-подібних шифрів / *В.І. Руженцев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 39 – 42.

Увага приділяється уточненню представлених в одній з попередніх робіт лемми та теореми стосовно ефективних байтових диференційних характеристик, які можуть бути використані в атаці усічених диференціалів. Представлено кореговане формулювання леми про граничну кількість активних колонок та нове доведення теореми про відсутність ефективних байтових диференційних характеристик в Rijndael-подібних шифрах. Виконується порівняння теоретично отриманих оцінок з отриманими на практиці результатами.

Табл. 1. Бібліогр.: 10 назв.

UDC 681.3.06: 519.248.681

About the proof of effective byte differential characteristics absence for Rijndael-like ciphers / *V.I. Ruzhentsev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 39 – 42.

The attention is paid to the correction of the lemma and theorem presented in the previous paper. These statements are about the effective byte differential characteristics which can be used in truncated differential

attack. The correction of formula of lemma about the boundary number of active columns and the new proof of theorem about effective byte differential characteristics absence for Rijndael-like ciphers is presented. The comparison of theoretical results and practical estimations is carried out.

1 tab. Ref.: 10 items.

УДК 681.3.06

Формирование нелинейных узлов замен с использованием недвоичных криптографических функций / *А.А. Кузнецов, А.В. Коваленко, С.А. Исаев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 43 – 57.

Исследуются математические модели регулярных нелинейных узлов замен (S-блоков) симметричных криптографических алгоритмов. Рассматривается традиционный подход, в котором для описания внутренней структуры S-блоков используется совокупность компонентных булевых функций. Исследуется аналитический аппарат недвоичных криптографических функций, с использованием которого разрабатывается математическая модель регулярных нелинейных узлов замен для формализации описания внутренней структуры S-блоков, развития методов их синтеза и оценки криптографических свойств. Приводятся результаты вычислительного поиска S-блоков с использованием предлагаемого математического аппарата, показано, что по нелинейности и автокорреляции сформированные узлы замен обладают улучшенными свойствами.

Табл. 4. Библиогр.: 14 назв.

УДК 681.3.06

Формування нелінійних вузлів замін з використанням недвійкових криптографічних функцій / *О.О. Кузнецов, О.В. Коваленко, С.О. Ісаєв* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 43 – 57.

Досліджуються математичні моделі регулярних нелінійних вузлів замін (S-блоків) симетричних криптоалгоритмів. Розглядається традиційний підхід, у якому для опису внутрішньої структури S-блоків використовується сукупність компонентних мулевих функцій. Досліджується аналітичний апарат недвійкових криптографічних функцій, з використанням якого розробляється математична модель регулярних нелінійних вузлів замін для формалізації опису внутрішньої структури S-блоків, розвитку методів їх синтезу та оцінки криптографічних властивостей. Доводяться результати обчислювального пошуку S-блоків з використанням пропонує мого математичного апарату, показано, що по нелінійності та автокореляції сформовані вузли замін володіють покращеними властивостями.

Табл. 4. Бібліогр.: 14 назв.

UDC 681.3.06

Synthesis of nonlinear substitution components with the use of non-binary cryptographic functions // *A.A. Kuznetsov, A.V. Kovalenko, S.A. Isaev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 43 – 57.

The mathematical model of regular nonlinear substitution components (S-blocks) of symmetric cryptographic algorithms is studied. The traditional approachis considered, in which the set of component Boolean functionsis used to describethe S-boxesinternal structure. The analytical apparatus of non-binary cryptographic functions with the use of which the mathematical model of regular nonlinear substitution component is developed to formalize the description of the internal structure of S-blocks, development of methods for their synthesis and evaluation of their cryptographic properties are investigated.The results of computational searchof S-blocks using the mathematical apparatus are shown, it is demonstrated that the nonlinearity and autocorrelation of the generated S-blocks have improved properties.

Tab.4. Ref.: 14 items.

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ
CRYPTOGRAPHIC TRANSFORMATION

УДК 004.056.55

Исследование методов вычисления инверсии в алгоритме NTRU / *Е.Г. Качко, Д.С. Балагура, К.А. Погребняк, Ю.И. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 58 – 63.

Цель работы – исследование различных методов вычисления инверсии, их оптимизация с учетом возможностей параллельных вычислений. Исследуются алгоритмы инверсии, приведенные в различных источниках как для инверсии в общем случае, так и для инверсии для модуля 2. Рассмат-

ривается возможность оптимизации указанных алгоритмов с точки зрения их возможной параллелизации. Показывается возможность существенного ускорения алгоритмов инверсии за счет их параллелизации и других методов ускорения алгоритмов.

Табл. 3. Ил. 1. Библиогр.: 5 назв.

УДК 004.056.55

Дослідження методів обчислення інверсії у алгоритмі NTRU / *О.Г. Качко, Д.С. Балагура, К.А. Погребняк, Ю.І. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 58 – 63.

Мета роботи – дослідження різноманітних алгоритмів обчислення інверсії, їх оптимізація з урахуванням можливостей паралельних обчислень. Досліджуються алгоритми інверсії, наведені у різних джерелах як для інверсії у загальному випадку, так і для інверсії для модуля 2. Розглядається можливість оптимізації зазначених алгоритмів з точки зору їх можливої паралелізації. Показується можливість суттєвого прискорення алгоритмів інверсії за рахунок їх паралелізації та інших методів прискоренні алгоритмів

Таб. 3 Іл. 1. Бібліогр. :5 найм.

UDC 004.056.55

Investigation of methods for calculation of the inversion algorithm, NTRU / *E.G. Kachko, D.S. Balagura, K.A. Pogrebnyak, Y.I. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 58 – 63.

The purpose of this article is to investigate different methods for calculating the inversion, to optimize them with the possibilities of parallel computing. The inversion algorithms presented in various sources for the inversion in the general case, and for the inversion for module 2 are studied. The possibility of the indicated algorithms optimization from the point of view of their possible parallelization is considered. The possibility of significant acceleration of inversion algorithms due to their parallelization, and other methods to accelerate algorithms is shown.

Tab 3. Fig.1. Ref.: 5 items.

УДК 681. 3.06

Криптографическая поддержка услуг защиты от несанкционированного доступа / *Ю.М. Леншина, А.В. Леншин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 64 – 71.

Проанализированы требования национальных и международных документов, регламентирующих защиту от несанкционированного доступа. Разработаны рекомендации по усовершенствованию НД ТЗИ в части спецификации услуг защиты от угроз приватности. Рассмотрены подходы к криптографической поддержке услуг защиты от несанкционированного доступа и методология оценки уровня стойкости услуг безопасности. Приведены условия обеспечения доказуемого уровня стойкости.

Табл. 5. Ил. 1. Библиогр.: 9 назв.

УДК 681. 3.06

Криптографічна підтримка послуг захисту від несанкціонованого доступу / *Ю.М. Лєншина, А.В. Лєншин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 64 – 71.

Проаналізовано вимоги національних та міжнародних документів, що регламентують захист від несанкціонованого доступу. Розроблено рекомендації з вдосконалення НД ТЗІ в частині специфікації послуг захисту від загроз порушення приватності. Розглянуті підходи до криптографічної підтримки послуг захисту від несанкціонованого доступу та методологія оцінки рівня стійкості послуг безпеки. Наведено умови забезпечення доказового рівня стійкості.

Таб. 5. Іл. 1. Бібліогр. : 9 назв.

UDC 681. 3.06

Cryptographic support of unauthorized access protection services / *I.M. Lyenshyna, A.V. Lyenshyn* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2012. N 171. P. 64 – 71.

The requirements of national and international instruments governing the protection from unauthorized access are analyzed. Recommendations for improving ND TZI services regarding the privacy protection are proposed. The approaches to the cryptographic support of unauthorized access protection services and evaluation methodology of its strength level are discovered. Conditions to provable strength of cryptographic support of privacy services are given

Tab.5. Fig. 1. Ref.: 9 items.

УДК 681.3.06

Модель использования облачных вычислений для задач асимметричного криптоанализа на примере факторизация чисел методом ρ-Полларда / *К.А. Погребняк, Д.В. Повтарев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 72 – 78.

Приводится анализ преимуществ и недостатков использования облачных вычислений для задач криптонализа, на основе которых формируется перечень требований к криптоаналитической системе. Разрабатывается общая модель использования облачных вычислений для задач асимметричного криптоанализа.

Приводится описание модуля, использующего облачные вычисления, и проводится анализ результатов его использования в сравнении с аналогичным решением, функционирующим на базе персонального компьютера.

Табл. 2. Ил. 2. Библиогр.: 7 назв.

УДК 681.3.06

Модель використання хмарних обчислень для задач асиметричного криптоаналізу на прикладі факторизації чисел методом ρ-Полларда / *К.А. Погребняк, Д.В. Повтарев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 72 – 78.

Наводено аналіз переваг та недоліків використання хмарних обчислень у задачах криптоналізу, на основі яких формується перелік вимог до криптоаналітичної системи. Описується розроблена загальна модель використання хмарних обчислень для задач асиметричного криптоаналізу.

Наводено опис розробленого модуля, що використовує ресурси на основі хмарних обчислень та проводиться аналіз результатів його використання у порівнянні з аналогічним рішенням, що функціонує на базі персонального комп'ютера.

Табл. 2. Іл. 2. Бібліогр.: 7 назв.

UDC 681.3.06

Model of using cloud computing for problems of asymmetric cryptanalysis illustrated by the example of factorization of numbers by ρ-Pollard algorithm / *K.A. Pogrebnyak, D.V. Povtariev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 72 – 78.

The main advantages and disadvantages of using the cloud computing for the problems of cryptanalysis were analyzed. The list of requirements for cryptanalytic system and general model based on it was designed according to the environment specific.

The program module of the cloud computing system for cryptanalysis tasks was developed and results of its usage were analyzed and compared with the same solution functioning on the PC basis.

Tab. 2. Fig. 2. Ref.: 7 items.

УДК 004.056.55

Анализ стойкости вычислительных задач, основанных на билинейных отображениях / *И.Д. Горбенко, Л.В. Макутонина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 79 – 89.

Одним из самых перспективных направлений развития криптосистем на идентификаторах является объединение математики спаривания точек на эллиптических кривых с алгебраическими решетками. Представлены определения и анализ основных вычислительных задач, основанных на билинейных отображениях, в последующих работах будет представлен анализ вычислительных задач на решетках, а также объединенной математики.

Библиогр: 17 назв.

УДК 004.056.55

Аналіз стійкості обчислювальних задач, що засновані на білінійних відображеннях / *І.Д. Горбенко, Л.В. Макутоніна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 79 – 89.

Одним із найперспективніших напрямів розвитку криптосистем на ідентифікаторах є об'єднання математики спарювання точок на еліптичній кривій з алгебраїчними решітками. У статті надано визначення та аналіз основних обчислювальних задач, що засновані на білінійних відображеннях, у наступних роботах буде надано аналіз обчислювальних задач на решітках, а також об'єднаної математики.

Бібліогр: 17 назв.

UDC 004.056.55

Resistance analysis computational problems based on the bilinear maps / *I.D. Gorbenko, L.V.Makutonina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 79 – 89.

At the moment, one of the most promising areas of identity-based cryptosystems is the union of mathematics pairings points on elliptic curves and algebraic lattices. This paper presents the definition and analysis of the major computing tasks based on bilinear maps. The subsequent works will analyze the computational problems on lattices and combined math.

Ref.: 17 items.

УДК 621. 391:519.2:519.7

Методы противодействия атакам специального вида на схемы направленного шифрования в кольцах срезанных полиномов / *Д.В. Иваненко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 90 – 98.

Анализируется методы противодействия атакам на реализацию, которые основываются на анализе энергопотребления. Рассматривается реализация схем направленного шифрования в кольце срезанных полиномов, принимая во внимания встраивания методов противодействия, таких как рандомизация и «заслепление». Были выявлены недостатки и преимущества методов противодействия относительно таких атак, как SPACPAи DPA, которые были направлены на схему направленного шифрования.

Табл.1 Ил. 5 Библ.: 19 назв.

УДК 621.391:519.2:519.7

Методи протидії атакам спеціального виду на схеми направленого шифрування у кільцях зрізаних поліномів / *Д.В. Іваненко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 90 – 98.

Аналізуються існуючі методи протидії атакам на реалізацію, які базуються на аналізі енергоспоживання. Розглядається реалізація схеми направленого шифрування, беручи до уваги впровадження методів протидії, таких яке рандомізація та засліплення. Було виявлено недоліки та переваги методів протидії відносно таких атак спеціального виду як SPA,CPA та DPA, які були направлені на схему направленого шифрування.

Табл. 1. Іл. 5. Бібл.: 19 назв.

UDC 621. 391:519.2”519.7

Methods to counteract side channel attacksto the schemes in rings of truncated polynomials / *D.V.Ivanenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 90 – 98.

The existing methods to counteract the attacks on the implementations based on the energy consumption analysis are considered. Realization of the directed encryption schemes in rings of truncated polynomials, given the embedding methods to counteract such as randomization and "blindness", is analyzed. The advantages and disadvantages of methods to counteract SPA CPA and DPA attacks sent to the directed encryption schemes are identified.

Tab1. Fig.5. Ref.: 19items.

УДК 681.3.06

Сущность и анализ криптографических требований стандарта NISTSP 800-90B / *И.Д. Горбенко, Р.И. Мордвинов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 99 – 108.

Одним из наиболее важных моментов в криптографии являются ключевые данные. Они должны удовлетворять ряду выдвигаемых к ним требований, одним из которых является случайность последовательности. Для удовлетворения данным свойствам, ключевые данные принято создавать с помощью генераторов случайной последовательности. В статье рассматривается стандарт, описывающий требования и методы тестирования таких генераторов и их компонентов.

Ил. 1. Библиогр: 1 назв.

УДК 681.3.06

Сутність та аналіз криптографічних вимог стандарту NISTSP 800-90B / *Ю.І. Горбенко, Р.І. Мордвінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 99 – 108.

Одним з найбільш важливих моментів у криптографії є ключові дані. Вони повинні задовольняти ряду вимог, що до них висуваються, одним з яких є випадковість послідовності. Для задовільнення даним вимогам, ключові дані прийнято створювати за допомогою генераторів випадкової

послідовності. В статті розглядається стандарт, в якому описані вимоги та методи тестування таких генераторів та їх компонентів.

Іл. 1. Бібліогр: 1 назв.

UDC 681.3.06

Essence and analysis of cryptographic requirements from NIST SP 800-90B / *U.I. Gorbenko, R.I. Mordvinov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 99 – 108.

Thekey dataare one of the mostimportant issuesin cryptography.They have tomeet a numberof requirementsput forwardto them, one of which is a randomsequence.To satisfythese properties it is a coomon practice rogeneratekey datausinga random sequencegenerator. Thestandard describingthe requirementsand test methods forsuchgenerators andtheir componentsn are considered.

1 fig. Ref.: 1 items.

УДК 681.3.06

Универсальное хеширование с ограничением функционального поля алгебраических кривых / *Е.В. Котух* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 109 – 115.

Представлено решение задачи построения универсального хеширования с ограничением функционального поля алгебраических кривых. Рассмотрены свойства хеширования по двум параметрическим базисам кривой Судзуки. Получены оценки вероятности коллизии, сложности вычислений и ключевого пространства для хеширования. Универсальное хеширование с ограничением функционального поля алгебраической кривой приводит к существенному снижению сложности вычислений. При этом уменьшается число хешируемых данных. Требуется оптимизация базиса функционального поля. Эффект достигается на сложных многопараметрических кривых.

Табл. 1. Библиогр.: 9 назв.

УДК 681.3.06

Універсальне гешування з обмеженням функціонального поля алгебраїчних кривих / *Є.В. Котух* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 109 – 115.

Представлено рішення задачі побудови універсального гешування з обмеженням функціонального поля алгебраїчних кривих. Розглянуто властивості гешування по двох параметричних базисах кривої Судзукі. Отримано оцінки ймовірності колізії, складності обчислень і ключового простору для хешування. Універсальне гешування з обмеженням функціонального поля алгебраїчної кривої призводить до істотного зниження складності обчислень. При цьому зменшується число гешированих даних. Потрібно оптимізація базису функціонального поля. Ефект досягається на складних багато параметричних кривих.

Табл. 1. Бібліогр.: 9 назв.

UDC 681.3.06

Universal hashing with limited functional field of algebraic curves / *Ye. Kotukh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 109 – 115.

The solution of the problem of constructing a universal hashing with limited functional field of algebraic curves is presented. The properties of the hashing on two-parametric basis of Suzuki curve are considered. Estimation of the collision probability, computational complexity and key space for hashing are obtained. Universal hashing with the limited function field of the algebraic curve results in a significant reduction in the computational complexity. It causes that the number of hash data is decreased. Optimization of the functional field basis is needed. Such effect can be achieved on complex multi-parameter curves.

Tab.1. Refs.: 9 titles.

УДК 004.056.55

Алгоритм решета числового поля / *И. Д. Горбенко, М.В. Есина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 116 – 122.

Определены особенности факторизации на основе общего алгоритма «решета числового поля», а также обоснован выбор факторных баз. Определён принцип построения алгебраической факторной базы и алгебраической базы характеров. Также определена оценка сложности решета числового поля.

Библиогр.: 5 назв.

УДК 004.056.55

Алгоритм решета числового поля / *І. Д. Горбенко, М. В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 116 – 122.

Визначено особливості факторизації на основі загального «решета числового поля», а також обґрунтовано вибір факторних баз. Визначено принцип побудови алгебраїчної факторної бази та ал-

гебраїчної бази характерів. Також визначена оцінка складності решета числового поля.

Бібліогр.: 5 назв.

UDC 004.056.55

Number field sieve algorithm / *I. D. Gorbenko, M. V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 116 – 122.

The major features of the factorization based on a total "number field sieve" are defined, and the choice of factor bases is justified. The principle of algebraic factor base and algebraic characters base are defined. The estimate of the number field sieve is determined as well.

Ref.: 5 items

УДК 004.056.55

Подходы к распараллеливанию программной реализации операции умножения целых чисел / *В.Ю.Ковтун, А.А.Охрименко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 123 – 131.

Рассматриваются подходы к повышению производительности программной реализации алгоритма умножения целых чисел для 32- и 64-разрядных платформ, посредством технологии распараллеливания. Основная идея распараллеливания алгоритма, состоит в использовании механизма отложенного переноса предложенного авторами ранее. Отложенный перенос позволяет избавиться от связности в итерациях циклов накопления суммы произведений, что позволяет выполнить их параллельно. После завершения потоков накопления суммы произведений, производится корректировка конечного результата посредством учета переносов. Такие подходы увеличивают общее число операций сложения, однако уменьшают общее время выполнения программной реализации на многопроцессорных и многоядерных вычислительных системах.

Табл. 1. Ил. 4. Библиогр.: 11 назв.

УДК 004.056.55

Підходи до розпаралелювання програмної реалізації операції множення цілих чисел / *В.Ю. Ковтун, А.О. Охріменко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 123 – 131.

Розглядаються підходи до підвищення продуктивності програмної реалізації алгоритму множення цілих чисел для 32- і 64-розрядних платформ, за допомогою технології розпаралелювання. Основна ідея розпаралелювання алгоритму полягає у використанні механізму відкладеного перенесення запропонованого авторами раніше. Відкладене перенесення дозволяє позбавитися від зв'язності в ітераціях циклів накопичення суми добутків, що дозволяє виконати їх паралельно. Після завершення потоків накопичення суми добутків, проводиться корегування кінцевого результату за допомогою врахування переносів. Такі підходи збільшують загальне число операцій додавання, однак зменшують загальний час виконання програмної реалізації на багатопроцесорних і багатоядерних обчислювальних системах.

Табл. 1. Іл. 4. Бібліогр.: 11 назв.

UDC 004.056.55

Approaches to parallelization of software implementation of integer multiplication / *V.Y. Kovtun, A.O. Okhrimenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 123 – 131.

Several approaches to the increasing performance of software implementation of integer multiplication algorithm for the 32-bit & 64-bit platforms via parallelization are considered. The main idea of algorithm parallelization consists in delayed carry mechanism using proposed by the authors earlier [11]. The delayed carry allows to get rid of connectivity in loop iterations for sums accumulation of products, which allows parallel execution of loops iterations in separate threads. After the finishing sum accumulation threads, it is necessary to make corrections in final result via carries considerations. First approach consists in parallelization optimization for the two execution threads and second approach is an evolution of the first approach and oriented on at most three execution threads. Proposed approaches for parallelization allows increasing the total algorithm computational complexity, as for one execution thread, but decrease total execution time on multi-core CPU.

1 tab. 4 fig. Ref.: 11 items.

УДК 004.056.5

Аутентификция аппаратных средств КЗИ / *А.А. Шевчук, Ю.И. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 132 – 139.

Рассматриваются уточнения в модели угроз средств КЗИ. Рассматривается влияние особенности использования ключей сессии в ЭЦП, основанные на схеме Ниберг – Рюпеля и DSA. Рассматривается

возможное влияние третьей стороны, участвуюшей в распространении средства. Предлагается обязательная аутентификация средств КЗИ, которые предоставляют услугу ЭЦП по определенным алгоритмам. Предлагается протокол аутентификации, с привлечением производителя средства.

Табл. 1. Библиогр.: 8 назв.

УДК 004.056.5

Автентифікація апаратних засобів КЗІ / *О.А. Шевчук, Ю.І. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 132 – 139.

Розглядаються уточнення до моделі загроз засобів КЗІ. Розглядається вплив особливості використання ключів сесії в ЕЦП, що ґрунтуються на схемі Ніберг – Рюпеля та DSA. Розглядається можливий вплив третьої сторони, що бере учать у розповсюдженні засобу. Пропонується обов'язкова автентифікація засобів КЗІ, що надають послугу ЕЦП за визначеними алгоритмами. Пропонується протокол автентифікації, с залученням виробника засобу.

Табл. 1. Библиогр.: 8 назв.

UDC 004.056.5

HSM Authentication / *O.A.Shevchuk, U.I. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 132 – 139.

Clarification of the HSM threat modelsis considered. The influence of the particular use of session keys in the digital signature schemes based on Nyberg-Ryupel and DSA algorithms can be used by an intruder. HSM authentication protocol is proposed to reduce threats.

Tab. 1. Refs.: 8 titles.

УДК 681.3.06

Универсальное хеширование по обобщенным кривым Гурвица / *О.Г. Халимов, А.Н. Герцог* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 140 – 146.

Представлено решение задачи построения кривых Гурвица с наибольшим отношением числа точек к роду на основе метода приведения к обобщенным кривым минимального рода с перебором значений наибольшего показателя степени кривой. Рассмотрены свойства метода приведения к обобщенным кривым Гурвица минимального рода, примеры построения кривых по делителям порядка поля. Показано, что предложенный метод расширяет множество кривых, так как определяет построение кривых по одному делителю порядка поля и в среднем в 7.46 раза быстрее по сравнению с перебором по наименьшему показателю степени кривой.

Библиогр.: 10 назв.

УДК 681.3.06

Універсальне гешування за узагальненими кривими Гурвіца / *О.Г. Халімов, О.М. Герцог* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 140 – 146.

Представлено рішення задачі побудови кривих Гурвіца з найбільшим відношенням числа точок до роду на основі методу приведення до узагальнених кривим мінімального роду з перебором значень найбільшого показника ступеня кривої. Розглянуто властивості методу приведення до узагальнених кривим Гурвіца мінімального роду, приклади побудови кривих по дільникам порядку поля. Показано, що запропонований метод розширює безліч кривих, оскільки визначає побудову кривих по одному дільнику порядку поля і в середньому в 7.46 рази швидше у порівнянні з перебором за найменшим показником ступеня кривої.

Бібліогр.: 10 назв.

UDC 681.3.06

Universal hashing by generalized Hurwitz curves / *O.G. Khalimov, A.N. Guetzog* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 140 – 146.

The solution of the problem of Hurwitz curves construction with the highest ratio of the number of points to the genus on the basis of the method of reduction to the generalized curves of minimum genus with listing of the curve greatest exponent values is presented. The properties of the method of reduction to the generalized Hurwitz curves of minimum genus, some examples of curves construction by divisor of the field order are considered. It is shown that the proposed method increases the number of curves, since it determines the construction of curves, one factor of the order of the field and on the average is 7.46 times faster as compared to the listing of the smallest exponent of the curve.

Ref.: 10 items.

.

УДК 621.391:519.2:519.7

Оценка стойкости направленного шифра NTRU к атаке с адаптивно подобранными шиф-

ротекстами / *А.П. Бубырь, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 147 – 151.

Представлены результаты исследования программной модели атаки с адаптивно подобранными шифротекстами на алгоритм направленного шифрования NTRU. Экспериментально определена зависимость вероятности ошибочного дешифрования сообщения от использванных общесистемных параметров. Установлено, что для гарантированного восстановления открытого текста без знания личного ключа достаточно иметь не более 30-40 криптограмм специального вида. Даны рекомендации по защите от подобных атак. Сделаны выводы о допустимых сферах применения данного алгоритма.

Ил. 3. Библиогр.: 3 назв.

УДК 621.391:519.2:519.7

Оцінка стійкості направленого шифру NTRUдо атаки з адаптивно підібраними шифротекстами / *А.П. Бубир, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 147 – 151.

Представлено результати дослідження програмної моделі атаки з адаптивно підібраними шифротекстами на алгоритм направленого шифрування NTRU. Експериментально визначена залежність ймовірності помилкового дешифрування повідомлення від використаних загальносистемних параметрів. Встановлено, що для гарантованого відновлення відкритого тексту без знання особистого ключа достатньо мати не більше, ніж 30-40 криптограм спеціального виду. Надано рекомендації щодо захисту від подібних атак. Зроблені висновки про допустимі сфери використання даного алгоритму.

Іл. 3. Бібліогр.: 3 назви.

UDC621.391:519.2:519.7

Evaluation of lattice-based public key algorithm NTRU resistance against adaptive chosen ciphertexts attack / *A.P. Bubyr, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 147 – 151.

Results of research intothe adaptive chosen ciphertexts attack's program model are given. Dependence of incorrect message recovery probability on the used system-wide parameters was defined experimentally. It was found that for the guaranteed recovery of plaintext without knowledge of the private key it is enough to have at most 30-40 cryptograms ofa special kind. Recommendations for the protection against these attacks are provided. The conclusions about the allowable scope of the algorithm are considered.

1fig.,Ref.: 3 items.

УДК 621.391:519.2:519.7

Анализ двух методов аутентификации человека для применения в электронном биометрическом паспорте / *К.А. Бугаенко, И.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 152 – 158.

Изучаются стандартные механизмы аутентификации личности по геометрии лица, по динамической подписи лица, их возможности, преимущества и недостатки. Проводится анализ методов аутентификации лица и предложения по их совершенствованию. Как и анализ по личной рукописной подписи, определение идентичности по фотографии в паспорте гражданина Украины относят к наиболее доступного и признанному методу распознавания личности. Применение двух методов аутентификации личности по биометрическим признакам геометрии лица и по рукописному (динамическом) подписи в паспорте гражданина Украины будут намного эффективнее, если применять их одновременно. Так как вероятность подделки биометрических данных уменьшается в несколько раз по сравнению с отдельным применением каждого из методов. Одновременно уменьшатся и ошибки как первого, так и второго рода, что приведет к повышению эффективности и надежности рассматриваемых двух методов.

Табл. 3. Ил.: 4. Библиогр.: 6 назв.

УДК 621.391:519.2:519.7

Аналіз двох методів автентифікації особи для застосування в електроному біометричному паспорті / *Х.А. Бугаєнко, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 152 – 158.

Вивчаються стандартні механізми автентифікації особи по геометрії обличчя, по динамічному підпису особи, їх можливості, переваги та недоліки. Та проводиться аналіз методів автентифікації особи та пропозиції з їх вдосконалення. Як і аналіз по особистому рукописному підпису, визначення ідентичності по фотографії в паспорті громадянина України відносять до найбільш доступного і визнаному методу розпізнавання особистості. Застосування двох методів для автентифікації особи по біометричним ознакам геометрії обличчя та по рукописному (динамічному) підписі в паспорті громадянина України будуть набагато ефективніші, якщо застосовувати їх одночасно. Так як ймовірність підробки біометричних даних зменшується в декілька разів в порівняні з окремим застосуванням ко-

жного з методів. Одночасно зменшаться й помилки як першого, так і другого роду, що призведе до підвищення ефективності і надійності розглянутих двох методів.

Табл. 3. Іл.: 4. Бібліогр.: 6 назв.

UDC 621.391:519.2:519.7

Analysis of two methods of a person authentication for the use in electronic biometric passports / *K.A. Bugaenko, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 152 – 158.

The standard authentication mechanisms of a person by the face geometry, dynamic signature of a person, their capabilities, advantages and disadvantages are considered. Analysis of the authentication methods and proposals for their improvement are given. Like the analysis by a personal handwritten signature, the identity definition by a photo in the passport of a citizen of Ukraine belongs to the most affordable and recognized methods of a person recognition. The use of two methods to authenticate a person by biometric characteristics and geometry of the face on the manuscript (dynamic) signature in the passport of a citizen of Ukraine will be much more effective if we use them simultaneously. The probability to falsify the biometric data is reduced several times as compared with the individual usage of each method. Simultaneously, the errors both of the first and the second kind are reduced, all these will result in higher efficiency and reliability of the considered two methods.

Tab.3. Fig.4. Ref.: 6 items

ПЕРЕДАЧА И ОБРАБОТКА ИНФОРМАЦИИ
INFORMATION TRANSMISSION AND PROCESSING

УДК 621.391:519.2:519.7

Анализ методов обезличивания персональных данных / *Ю.И. Горбенко, А.С. Тоцкий, В.А. Пономарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 159 – 163.

Проанализировано методы обезличивания данных, которые удовлетворяют требованиям защиты персональных данных. Приведен алгоритм одного из методов и предложены разные варианты его реализации с соответствующими приоритетами: быстродействие, используемая память, сохранение необходимых статистических свойств.

Табл. 3. Библиогр.: 5 назв.

УДК 621.391:519.2:519.7

Аналіз методів знеособлення персональних даних / *Ю.І. Горбенко, О.С. Тоцький, В.А. Пономар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 159 – 163.

Проаналізовано методи знеособлення даних, які задовольняють вимогам захисту персональних даних. Наведено алгоритм одного з методів та запропоновані різні варіанти його реалізації з відповідними пріоритетами: швидкодія, необхідна пам’ять та збереження необхідних статистичних властивостей.

Табл. 3. Бібліогр.5 назв.

UDC 621.391:519.2:519.7

Analysis of the methods of personal data anonymization / *Y.I. Gorbenko, A.S. Totsky, V.A. Ponomar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 159 – 163.

The data anonymization techniques, which satisfy the requirements of the protection of personal data, is analyzed. An algorithm of one of the methods is given and different options for its implementation are proposed with the relevant priorities: performance, memory usage, conservation of the necessary statistical properties.

3 tab. Ref.: 5 items.

УДК 681.3.06

Модель институционального управления деятельностью по защите информации / *А.В. Потий, Д.Ю. Пилипенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 164 – 170.

Предлагается модель институционального управления деятельностью по защите информации. Проведено онтологическое моделирование института информационной безопасности и предметной области культуры информационной безопасности. Рассмотрены ключевые субъекты деятельности по защите информации: центр безопасности и агент безопасности. Установлены связи между субъектами деятельности по защите информации и компонентами модели.

Ил. 2. Библиогр.: 4 назв.

УДК 681.3.06

Модель інституціонального управління діяльністю із захисту інформації / *О.В. Потій, Д.Ю. Пилипенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 164 – 170.

Запропоновано модель інституціонального управління діяльністю із захисту інформації. Проведено онтологічне моделювання інституту інформаційної безпеки та предметної області культури інформаційної безпеки. Розглянуто головні суб'єкти діяльності із захисту інформації: центр безпеки та агента безпеки. Встановлено зв'язок між суб'єктами діяльності із захисту інформації та компонентами моделі.

Іл. 2. Бібліогр.: 4 назви.

UDC 681.3.06

Institutional model of information security activities management / *A.V. Potiy, D.Y. Pilipenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 164 – 170.

An institutional model of information security activities management is proposed. An ontological modeling of information security institution and subject domain of information security culture is carried out. The main subjects of information security activities are considered, namely the security center and security agent. The interconnections between the subjects of the information security activities and other components of this model are established.

2 fig. Ref.: 4 items.

УДК 681.323

Количественная оценка уязвимостей информационно-телекоммуникационных систем / *А.А. Замула, С.А.Сирота, Н.И. Косиковская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 171 – 176.

Проведен анализ архитектуры информационных систем, уязвимостей, которые присущи данным системам, и которые могут быть использованы злоумышленниками при проведении атак на такие системы. Получена математическая модель оценки уязвимостей информационно-телекоммуникационных систем.

Библиогр.: 3 назв.

УДК 681.323

Кількісна оцінка вразливостей інформаційно-телекомунікаційних систем / *О.А.Замула, С.О. Сирота, Н.І. Косіковська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 171 – 176.

Проведений аналіз архітектури інформаційних систем, вразливостей, які можуть бути притаманні даним системам, і які можуть бути використані зловмисниками при реалізації атак на такі системи. Отримана математична модель оцінки вразливостей інформаційно-телекомунікаційних систем.

Бібліогр.:3 назв.

UDC 681.323

Quantitative assessment of information technology systems vulnerabilities / *O.A.Zamula, S.O.Syrota, N.I.Kosikovskaia* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 171 – 176.

The analysis of information systems architecture, vulnerabilities that are inherent in these systems, and that can be used by intruders to conduct attacks on such systems was carried out. The mathematical model of vulnerability assessment of information technology systems was obtained.

Ref.: 3 items.

УДК 621.391

Предложения по построению широкополосных систем передачи со сложными сигналами / *А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 177 – 184.

Сформулирована задача выбора сложных сигналов для широкополосных систем передачи. Определены необходимые и достаточные условия построения абсолютно стойкой системы передачи на уровне источника сложных сигналов

Ил. 3. Библиогр.: 4 назв.

УДК 621.391

Пропозиції щодо побудови широкополосних систем передачі зі складними сигналами / *О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 177 – 184.

Сформульовано задачу відбору складних сигналів для широкополосних систем передачі інформації. Визначені необхідні та достатні умови побудови абсолютно стійких систем передачі на рівні джерела складних сигналів.

Іл. 3. Бібліогр.: 4 назв.

UDC 621.391

Proposal for construction of the wide-band transmission systems with complex signals / *O.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 177 – 184.

The task of choosing complex signals for wideband transmission systems is formulated. The necessary and sufficient conditions for constructing transmission systems that are completely resistant on the level of complex signals' source are defined.

3 fig. Ref.: 4 items.

УДК 004.056.5: 004.775

Синтез системы многоуровневой защиты корпоративных порталов на платформе MS SHARE POINT / *Б.О. Бабич, А.В. Сагун, О.А. Кожуховская, А.Д. Кожуховский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 185 – 188.

Рассмотрены вопросы безопасности корпоративных порталов, современные тенденции, предложено практическое решение системы защищённого корпоративного портала на базе многоуровневой системы защиты корпоративных порталов платформы MS Share Point при помощи интегрируемого программного обеспечения Microsoft. Представлена универсальная тестовая топология для изучения алгоритма построения защищенной облачной системы.

Ил.2 . Библиогр.: 7 назв.

УДК 004.056.5: 004.775

Синтез системи багаторівневого захисту корпоративних порталів на платформі MS SHARE POINT / *Б.О. Бабич, А.В. Сагун, О.А. Кожухівська, А.Д. Кожухівський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 185 – 188.

Розглянуто питання безпеки корпоративних порталів, сучасні тенденції і одне із практичних рішень. Досліджено питання побудови багаторівневої системи захисту корпоративних порталів на платформі MS SHARE POINT за допомогою інтегруємого програмного забезпечення Microsoft. Представлена універсальна тестова топологія для вивчення алгоритму побудови захищеної хмарової системи.

Ключові слова: корпоративний портал, хмарові системи, безпека, багаторівневий захист, Share Point.

Іл. 2. Бібліогр.: 7 назв.

UDC 004.056.5: 004.775

Synthesis of system of multilevel protection of corporate portals on the base of Share Point Platform / *B.A. Babich, A.V. Sagun, O.A. Kozhukhovska, A.D. Kozhukhovskiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 185 – 188.

The problems of corporate portals' safety, modern trends and a practical solution were considered. The problems of building a multilevel system of corporate portals' protection on the base of MS Share Point Platform with the help of integrated Microsoft Software were investigated. The universal test topology for studying the algorithm of building up the protected cloudy system was presented.

Fig.2. Ref.: 7 items.

УДК 621.396

Критерии и показатели эффективности стеганографических систем защиты информации / *А.А. Смирнов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 189 – 197.

Рассматривается задача стеганографической защиты информации, основной целью которой является сокрытие не только смыслового содержания передаваемых данных, но и самого факта осуществления скрытной передачи. Исследуется математическая модель и структурная схема стеганографической системы. Вводятся основные операторы, формально описывающие основные вычислительные процессы при стенографическом преобразовании информации на передающей и принимающей стороне. Вводятся критерии и показатели эффективности функционирования стеганографической системы. В общем виде формализуется задача совершенствования стеганосистемы через максимизацию обобщенного показателя ее эффективности.

Ил. 3. Библиогр.: 10 назв.

УДК 621.396

Критерії й показники ефективності стеганографічних систем захисту інформації / *А.А. Смірнов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 189 – 197.

Розглядається завдання стеганографічного захисту інформації, основною метою якого є приховання не тільки визначеного змісту переданих даних, але й самого факту здійснення потайливої пере-

дачі. Досліджується математична модель і структурна схема стеганографічної системи. Уводяться основні оператори, що формально описують основні обчислювальні процеси при стенографічному перетворенні інформації на передавальній і приймаючій стороні. Уводяться критерії й показники ефективності функціонування стеганографічної системи. У загальному виді формалізується завдання вдосконалювання стеганосистеми через максимізацію узагальненого показника її ефективності.

Іл. 3. Бібліогр.: 10 назв.

UDC 621.396

Criteria and indexes of efficiency of the steganography systems of priv / *A.A. Smirnov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 189 – 197.

The task of steganography priv, the primary purpose of which is a concealment not only of semantic maintenance of transferrable information but also the fact of realization of secretive transmission is examined. A mathematical model and flow diagram of the steganography system is probed. Basic operators are entered, legalistically describing basic calculable processes at stenographic transformation of information on the transmitting and receiving side. Criteria and indexes of efficiency of functioning of the steganography system are introduced. In a general view the task of perfection of steganosystems is formalized through maximization of the generalized index of its efficiency.

Fig.: 3. Ref.: 10 items.

УДК 621.391.7:336.71(075.8)

Сравнительный анализ протоколов строгой аутентификации / *И.В. Олешко, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 198 – 209.

Оцениваются протоколы строгой аутентификации на основании условных и безусловных критериев. Показывается, что наилучшим протоколом аутентификации является протокол, основанный на сертификатах с использованием преобразований в группе точек эллиптической кривой.

Табл. 1. Ил. 7. Библиогр.: 9 назв.

УДК 621.391.7:336.71(075.8)

Порівняльний аналіз протоколів суворої автентифікації / *І.В. Олешко, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 198 – 209.

Проводиться оцінка протоколів суворої автентифікації на основі умовних і безумовних критеріїв. Показано, що найкращим протоколом автентифікації є протокол, заснований на сертифікатах з використанням перетворень в групі точок еліптичної кривої.

Табл. 1. Іл. 7. Бібліогр.: 9 назв.

UDC 621.391.7:336.71(075.8)

Comparative analysis of strong authentication protocols / *I.V. Oleshko, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 198 – 209.

The estimate of the strong authentication protocol based on conditional and unconditional criteria is carried out. It is shown that the best authentication protocol is the protocol based on the certificate with transformations in the group of the elliptic curve points.

Tab.1. Fig.7. Ref.:9 items.

РАДИОЛОКАЦИЯ
RADAR

УДК 621.396:621.391.82

Пространственная селекция широкополосных источников по собственным числам ковариационной матрицы / *О.В. Сытник, В.М. Карташов, А.А. Супрун* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С.210 – 215.

Рассматривается статистически оптимальный алгоритм пространственно-временной обработки сигналов для селекции точечных источников шумовых сигналов. В основу алгоритма положено представление пространственно-временной ковариационной матрицы наблюдения в виде набора матриц, полученных из усредненных сигналов многоотводных линий задержки приемных каналов адаптивной антенной решетки. Это позволило непосредственно по анализу собственных чисел строить оценки углового положения источников. Обработка сигнала при этом выполняется в несколько этапов, включающих оценивание пространственно-временной ковариационной матрицы по сигналам каналов приема, вычисления ее собственных чисел их ранжирования и оценивания соответствующих весовых коэффициентов матрицы усилителей. Выигрыш в чувствительности по отношению к клас-

сическому способу обработки в значительной мере зависит от допустимого интервала наблюдения, на котором осуществляется прием сигналов.

Библиогр.:10 назв.

УДК 621.396:621.391.82

Просторова селекція широкосмугових джерел за власними числами коваріаційної матриці / *О.В. Ситнік, В.М.Карташов, О.О. Супрун* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С.210 – 215.

Розглядається статистично оптимальний алгоритм просторово-часової обробки сигналів для селекції точкових джерел шумових сигналів. В основу алгоритму покладено уявлення про просторово-часову коваріаційну матрицю спостереження у вигляді набору матриць, отриманих з усереднених сигналів багатовідвідної ліній затримки приймальних каналів адаптивної антенної решітки. Це дозволило безпосередньо з аналізу власних чисел будувати оцінки кутового положення джерел. Обробка сигналу при цьому виконується в кілька етапів, що включають оцінювання просторово-часової коваріаційної матриці за сигналами каналів прийому, обчислення її власних чисел подальше їх ранжування та оцінювання відповідних вагових коефіцієнтів матриці підсилювачів. Виграш в чутливості по відношенню до класичного способу оброблення в значній мірі залежить від допустимого інтервалу спостереження, на якому здійснюється прийом сигналів.

Бібліогр.: 10 назв.

UDC 621.396:621.391.82

Spatial selection of wide-band sources using eigenvalue of the covariance matrix / *O.V. Sytnik, V.M.Kartashov, O.O. Suprun* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 210 – 215.

The statistically optimal space-time signal processing algorithm for the point sources selection of noise signals is considered. The representation of the space-time covariance observation matrix as a set of matrices obtained from the averaged signals of the multipoint delay lines of the adaptive antenna array receiving channels is used as the algorithm basis. This makes it possible to construct the angular position estimates of the sources on the eigenvalue analysis. The signal processing in this case includes the space-time covariance matrix estimation by the signals of the receiving channels, the eigenvalues calculation of the space-time covariance matrix, the ranking calculation of eigenvalues, the corresponding coefficients estimation of the amplifier matrix. The gain in the sensitivity in relation to the classical processing method depends mainly on the tolerance observation interval during which the signals are received.

Ref.: 10 items.

УДК 621.396

Расчет характеристик обнаружения сигналов, отраженных объектами, расположенными на морской поверхности, полуактивной бистатической РЛС с цифровым телевизионным сигналом подсвета / *А.А. Байздренко, В.Б. Лубский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 216 – 221.

Многочисленные исследования в области полуактивных бистатических РЛС с телевизионным подсветом подтвердили потенциальную возможность использовать телевизионный сигнал для радиолокационного обнаружения воздушных целей. Телевизионный сигнал по своим энергетическим характеристикам пригоден для обнаружения объектов также и на морской поверхности. Специфика распространения радиоволн над морской поверхностью требует разработки соответствующих методик расчетов характеристик обнаружения сигналов, отраженных морскими целями. Авторами статьи предлагается вариант расчетов характеристик обнаружения сигналов, отраженных объектами, расположенными на морской поверхности, бистатической РЛС с цифровым телевизионным сигналом подсвета.

Ил. 1. Библиогр.: 21 назв.

УДК 621.396

Розрахунок характеристик виявлення сигналів, відбитих об'єктами, розташованими на морській поверхні, полуактивною бістатичною РЛС з цифровим телевізійним сигналом освітлення / *О.О. Байздренко, В.Б. Лубський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 216 – 221.

Численні дослідження у галузі полуактивних бістатичних РЛС з телевізійним освітленням підтвердили потенційну можливість застосовувати телевізійний сигнал для радіолокаційного виявлення повітряних цілей. Телевізійний сигнал за своїми енергетичними характеристиками придатний для виявлення об'єктів також і на морський поверхні. Специфіка розповсюдження радіохвиль над морською поверхнею вимагає розробку відповідних методик розрахунків характеристик виявлення сигналів, відбитих морськими цілями. Авторами статті пропонується варіант розрахунку характеристик вияв-

лення сигналів, відбитих об’єктами, розташованими на морський поверхні, бістатичною радіолокаційною станцією з цифровим телевізійним сигналом освітлення.

Іл. 1. Бібліогр.: 21 назв.

UDC 621.396

Calculation of detection characteristics of signals, reflected by objects located on the sea surface, in semi-active bistatic radar with digital TV signal illumination / *A.A. Baizdrenko, V.B. Lubsky* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 216 – 221.

Numerous studies in the field of semi-active bistatic radars with television illumination confirmed the potential to use the TV signal for the radar detection of air targets. TV signal due to its energy performance is also suitable for detection of objects on the sea surface. Specificity of radio wave propagation over the sea surface requires the development of appropriate methods of calculation of the detection characteristics of the signals reflected by sea targets. A version of such calculations is presented.

1 fig. Ref.:21 items.

УДК 621.396.2

Сравнительный анализ помехозащищенности и спектральной эффективности Wi-Fi каналов связи с линейными и двумерными адаптивными антенными решетками при воздействии нескольких помех и одного сигнала / *А.А. Буланый, Г.В. Майстренко, А.А. Стрельницкий, В.М. Шокало* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 222 – 228.

Для частного случая прихода сигнала с направления близкого к нормали адаптивной антенной решетки (ААР) проведен сравнительный анализ помехозащищенности (уровень BER) и спектральной эффективности (СЭ) рэлеевских Wi-Fi каналов связи с линейными и двумерными ААР при воздействии нескольких помех и одного сигнала. Исследовались линейная и квадратная ААР, состоящие из четырех излучателей. Показано, что при воздействии одной помехи канал связи с квадратной решеткой по параметрам BER и СЭ существенно выигрывает по сравнению со случаем применения линейной ААР. Если же количество помех равно двум или трем, то более эффективным является канал с линейной решеткой. Определены значения отношения сигнал/помеха на входе ААР, при которых в канале связи может быть достигнуто высокое качество передачи информации.

Табл. 6. Ил. 4. Библиогр.: 6 назв.

УДК 621.396.2

Порівняльний аналіз завадозахищеності і спектральної ефективності Wi-Fi каналів зв'язку з лінійними та двовимірними адаптивними антенними решітками при впливі декількох завад і одного сигналу / *О.А. Буланий, Г.В. Майстренко, О.О. Стрельницький, В.М. Шокало* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 222 – 228.

Для частного випадку приходу сигналу з напрямку близького до нормалі адаптивної антенної решітки (ААР) проведено порівняльний аналіз завадозахищеності (рівень BER) і спектральної ефективності (СЕ) релєєвських Wi-Fi каналів зв'язку з лінійними та двовимірними адаптивними антенними решітками (ААР) при впливі декількох завад і одного сигналу. Досліджувалися лінійна і квадратна ААР, що складаються з чотирьох випромінювачів. Показано, що при впливі однієї завади канал зв'язку з квадратною решіткою по параметрам BER і СЕ виграє в порівнянні з випадком застосування лінійної ААР. Якщо ж кількість завад дорівнює двом або трьом, то ефективнішим є канал з лінійною решіткою. Визначено значення відносини сигнал/завада на вході ААР при яких в каналі зв'язку може бути досягнуто високу якість передачі інформації.

Табл. 6.Іл. 4. Бібліогр.: 6 назв.

UDC 621.396.2

Comparative analysis of immunity and spectral efficiency of Wi-Fi channels with linear and two-dimensional adaptive antenna array under the influence of several interferences and a signal / *A.A. Bulany, G.V. Maistrenko, A.A. Strelnitsky, V.M. Shokalo* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 222 – 228.

A comparative analysis of noise immunity (BER level) and spectrum efficiency (SE) of Rayleigh Wi-Fi channels with linear and two-dimensional adaptive antenna arrays (AAA) under the influence of several interferences and a signal is conducted for the particular case when the signal arrives from the direction near to the normal of AAA. Linear and square AAA consisting of four emitters are studied. It is demonstrated that under one interference action the communication channel with a square lattice according to the BER and SE parameters benefits significantly as compared to the case of the linear AAA application. The channel with a

linear array is more efficient if the amount of interferences is two or three. The values of the signal/noise ratio at the AAA input, wherein a high quality of information transmission can be attained, are defined.

6 tab. 4 fig. Ref.: 6 items.

УДК 621.376

Исследование ФАР с диэлектрическим заполнениемем и согласующей периодической структурой / *С.В Марченко, В.М Морозов., А.М. Съянов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 229 – 233.

Приведены результаты исследования бесконечной линейной волноводной ФАР для случая сканирования в Н-плоскости. Электродинамический алгоритм построен на основе метода пронизывающей области, который приводит к интегральному уравнению Фредгольма второго рода. Представлены численные результаты влияния параметров диэлектрического заполнения и размеров согласующей периодической структуры на согласование ФАР.

Ил. 6. Библиогр.: 4 назв.

УДК 621.376

Дослідження ФАР з діелектричним заповненням та узгоджуючою періодичною структурою / *С.В.Марченко, В.М Морозов, О.М. С'янов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С.229 – 233.

Наведено результати дослідження нескінченої лінійної хвилеводної ФАР для випадку сканування в Н-площині. Електродинамічний алгоритм побудовано на основі методу області, що пронизує, який призводить до інтегрального рівняння Фредгольма другого роду. Представлено чисельні результати впливу параметрів діелектричного заповнення та розмірів узгоджуючої періодичної структури на узгодження ФАР.

Іл. 6. Бібліогр.: 4 назв.

UDC 621.376

Investigation of PAA with dielectrical inclusion and matching periodical structure/ *S.V. Marchenko, V.M Morozov., A.M Syanov* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 229 – 233.

Results of investigation into the infinite linear waveguide PAA in the case of scanning in H-plane are presented. The electrodynamical algorithm is formulated on the basis of the penetrating area method which results in the second kind Fredholm equation. Numerical results of the dielectric inclusion and matching periodical structure parameters action on the PAA matching are presented.

6 fig. Ref.: 4 items.

УДК 551.501.8:621.396.96

Синтез и анализ дискриминатора следящего устройства систем радиоакустического зондирования атмосферы / *В.М. Карташов, Д.Н. Куля* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С.234 – 238.

Проанализированы особенности распространения радиоволн в условиях неоднородности атмосферы, искусственно вызванной акустическими колебаниями. Рассмотрены методы обработки отраженного радиосигнала от акустической посылки, позволяющие оценить температуру воздуха, и проанализированы причины погрешностей возникающих при обработке сигнала. Предложен корреляционный способ обработки, который обеспечивает высокую инструментальную точность регистрации вертикальных профилей температуры воздуха при сравнительно простом устройстве обработки рассеянных сигналов, где простота достигается главным образом за счет работы системы в режиме слежения за параметром расстройки условия Брэгга. Особенностью устройства является использование значения оцениваемого параметра, определенного на предыдущем цикле наблюдения.

Ил. 4. Библиогр.: 5 назв.

УДК 551.501.8:621.396.96

Синтез та аналіз дискримінатора слідкуючого пристрою систем радіоакустичного зондування атмосфери / *В.М. Карташов, Д.М. Куля* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 234 – 238.

Зроблено аналіз особливостей розповсюдження радіохвиль в умовах неоднорідності атмосфери, штучно викликаної акустичними коливаннями. Зроблено огляд методів обробки відбитого радіосигналу від акустичної посилки, що дозволяють оцінити температуру повітря та проаналізовані причини виникаючих похибок під час обробки сигналу. Запропоновано кореляційний спосіб обробки, котрий забезпечує високу інструментальну точність реєстрації вертикальних профілів температури повітря

при порівняно простому пристрої обробки розсіяних сигналів, де простота досягається за рахунок роботи системи в режимі слідкування за параметром розстройки умови Брега, особливістю котрого є використання значення параметра, визначеного на попередньому циклі спостереження.

Іл. 4. Бібліогр.: 5 назв.

UDC 551.501.8:621.396.96

Synthesis and analysis of the tracker device discriminator of the atmosphere radio acoustic sensing systems / *V.M.Kartashov, D.M.Kulia* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 234 – 238.

Features of the radio waves propagation in the atmosphere inhomogeneity induced by the acoustic vibrations are analyzed. Processing methods of the reflected radio signal from the speaker packages making it possible to estimate the air temperature are discussed. Causes of errors arising in the signal processing are analyzed. There is discussed the correlation processing method that provides high instrument accuracy of the vertical profiles registration of the air temperature at a relatively simple processing device of the scattered signals. Simplicity of the device is achieved by the operation of the system in the tracking mode for the parameter of the Bragg condition detuning. A feature of the device is to use the estimated parameter value defined in the previous cycle of observation.

4 fig. Ref.: 5 items.

УДК: 681.128.82

Контроль уровня легкоиспаряющихся жидкостей методом акустической локации / *Б.В. Жуков, А.В. Одновол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 239 – 244.

Представлены результаты экспериментальных исследований функционирования акустических уровнемеров с абсолютным и относительным методами измерения в процессе контроля уровня нескольких типов жидкостей. Они показали, что на результаты контроля уровня легкоиспаряющихся жидкостей оказывают влияние их пары, которые локализуются непосредственно над поверхностью.

Табл. 1 Ил. 6. Библиогр.: 4 назв.

УДК: 681.128.82

Контроль рівня легковипаровуючих рідин методом акустичної локації / *Б.В. Жуков, А.В. Одновол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 239 – 244.

Представлено результати експериментальних досліджень функціонування акустичних рівнемірів з абсолютним та відносним методами вимірювання в процесі контролю рівня декількох типів рідин. Вони показали, що на результати контролю рівня легковипаровуючих рідин впливають їх пари, які локалізуються безпосередньо над поверхнею.

Табл.1. Іл.6. Бібліогр.: 4 назв.

UDC 681.128.82

Control over the level of easily evaporated liquids by the acoustic location method / *B.V. Zhukov, A.V. Odnovol* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P.239 – 244.

Results of experimental researches of acoustic level meters functioning with absolute and relative measurement methods in the process of several types of liquids' level monitoring are presented. They showed that the vapors of the easily evaporated liquids localized directly above their surface act on the results of their level control.

1 tab. 6 fig. Ref.: 4 items.

УДК 535.+543.47+621.396

Об аналитических методах синтеза поляризационного эллипса / *Г.М. Чекалин, Г.Н. Чекалина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С.245 – 251.

Статья посвящена исследованию влияния исходной ориентации эллипса поляризации электромагнитной волны на вид аналитических выражений компонент поля и их разности фаз, а также коэффициента эллиптичности r и угла ориентации β при повороте системы отсчета на угол $\pm\beta$.

Ил. 3. Библиогр.: 3.

УДК 535.+543.47+621.396

Про аналітичні методи синтезу поляризаційного еліпса / *Г.М. Чекалін, Г.М. Чекаліна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 245 – 251.

Стаття присвячена дослідженню впливу вихідної орієнтації еліпса поляризації електромагнітної хвилі на вигляд аналітичних виразів компонент поля і їх різниці фаз, а також коефіцієнта еліптичності r і кута орієнтації β при повороті системи відліку на кут $\pm\beta$.

Іл. 3. Бібліогр.: 3.

UDC 535.+543.47+621.396

About analytical methods for synthesis of the polarization ellipse / *G.M. Chekalin, G.N. Chekalina* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 245 – 251.

The action of the polarization ellipse initial orientation of the electromagnetic wave on the analytic expressions form of the field components and their phase difference, and the coefficient of ellipticity r and orientation angle β, when rotating the reference frame at the angle $\pm\beta$, is investigated.

3 fig. Ref.: 3/

УДК 004.056

Результаты экспериментального исследования телефонных радиозакладных уст ройств методом нелинейной локации / *Ю.В. Лыков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 252 – 257.

Исследован метод нелинейной локации применительно к поиску радиозакладных устройств в проводных телефонных линиях. Разработаны требования к нелинейному локатору. Экспериментально получены нелинейные свойства некоторых моделей телефонных радиозакладных устройств. Показаны потенциальные возможности данного метода.

Ил. 7. Библиогр.: 4 назв.

УДК 004.056

Результати експериментального дослідження телефонних радіозакладних пристроїв методом нелінійної локації / *Ю.В. Ликов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 252 – 257.

Досліджено метод нелінійної локації стосовно до пошуку радіозакладних пристроїв в проводових телефонних лініях. Розроблено вимоги до нелінійного локатора. Експериментально отримані нелінійні властивості деяких моделей телефонних радіозакладних пристроїв. Показані потенційні можливості даного методу.

Іл. 7. Бібліогр.: 4 назв.

UDC 004.056

Results of experimental study of telephone radio bugs using nonlinear locations method / *Y.V. Lykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 252 – 257.

The method of nonlinear location for search of radio bugs in wired telephone lines is studied. The requirements to the nonlinear locator are developed. The nonlinear properties of some phones' radio bugs are obtained experimentally. The potentialities of this method are shown.

7 fig. Ref.: 4 items.

УДК 551.501.7

Модельно-структурный анализ эхосигналов акустического зондирования атмосферы / *В.И. Леонидов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 258 – 261.

Исследуются реализации акустических эхосигналов полученных на действующей станции акустического зондирования установленной в центре мегаполиса. Анализ проводится с помощью разрабатываемой методики модельно-структурного анализа, при которой моделируются эхосигналы, обусловленные структурными элементами турбулентного поля температуры.

Ил. 4. Библиогр.: 2 назв.

УДК 551.501.7

Модельно-структурний аналіз ехосигналів акустичного зондування атмосфери / *В.І. Леонідов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 258 – 261.

Досліджуються реалізації акустичних ехосигналів отриманих на діючій станції акустичного зондування встановленої в центрі мегаполіса. Аналіз проводиться за допомогою розроблювальної методики модельно-структурного аналізу, при якому моделюються ехосигнали, обумовлені структурними елементами турбулентного поля температури.

Іл. 4. Бібліогр.: 2 назв.

UDC 551.501.7

Model-structural analysis of echo signals of atmospheric acoustic sounding / *V.I. Leonidov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 258 – 261.

Realizations of the acoustic echo signals received at the working station of acoustic sounding and installed in the center of megalopolis are analyzed. The analysis is carried out using the structural-modeling analysis method, which is being presently developed and in accordance with which the echo signals stipulated by the structural elements of the temperatures turbulent field are modeled.

4 fig. Ref.: 2 items.

СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ
INFORMATION PROCESSING SYSTEMS

УДК 621.391

Разработка рекомендаций по регулированию пропускной способности в WPAN / *И.С. Шостко, Ю.Э. Соседки, Алмакадма Таха* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 262 – 269.

Для увеличения скорости передачи данных в радиоканале и обеспечения высокой помехоустойчивости в условиях многолучевого распространения и воздействия помех необходимо в перспективных системах WPAN использовать технологию UWB Multiband OFDM при оптимальном управлении параметрами сигнала. Для оценки показателей качества сверхширокополосных беспроводных систем связи, разработана модель приёмо-передатчика с использованием данной технологии. Модель позволяет исследовать: зависимости вероятности битовой ошибки от скорости свёрточного кодирования, от особенностей канала связи, от расстояния между приёмником и передатчиком и зависимость вероятности битовой ошибки от размера символа OFDM.

Ил. 10. Библиогр: 8 назв.

УДК 621.391

Розробка рекомендацій щодо регулювання пропускної здатності в WPAN / *І.С. Шостко, Ю.Е. Сосєдка, Алмакадма Таха* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 262 – 269.

Для збільшення швидкості передачі даних в радіоканалі і забезпечення високої завадостійкості в умовах багатопроменевого поширення і впливу перешкод необхідно в перспективних системах WPAN використовувати технологію UWB Multiband OFDM при оптимальному керуванні параметрами сигналу. Для оцінки показників якості надширокосмугових безпровідних систем зв'язку, розроблена модель прийомо-передавача з використанням даної технології. Модель дозволяє досліджувати: залежності ймовірності бітової помилки від швидкості згортального кодування, від особливостей каналу зв'язку, від відстані між приймачем і передавачем і залежність імовірності бітової помилки від розміру символу OFDM.

Іл. 10. Бібліогр.: 8 назв.

UDC 621.391

Development of recommendations concerning adjustment of carrying capacity in WPAN / *I.S. Shostka, J.E Sosedka, Almakadma Taha* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 262 – 269.

To increase the data transmission speed in the radio channel and to provide high immunity on the multipath dissemination condition and on the interference impact condition it is necessary in the perspective WPAN systems to use the UWB Multiband OFDM technology for the signal parameter optimum management. To assess the quality of UWB wireless communication systems, a model transceiver using this technology is developed. The model makes it possible to investigate the bit error probability dependence on the rate convolutional coding, the communication channel features, the distance between the receiver and the transmitter, the size of the OFDM symbol.

10 fig. Ref.: 8 items

УДК 621.391.23

Особенности передачи данных по блокам в транкинговой системе стандарта APCO 25 / *И.В. Ковтун* // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 270 – 274.

Рассмотрена сравнительная характеристика основных перспективных стандартов цифровой транкинговой связи TETRA, APCO 25 и TETRAPOL по эксплуатационно-техническому и организационно – экономическому критериям. Проведена оценка объема передачи данных по блокам в стан-

дарте APCO 25. Рассчитано время передачи данных для блоков с двумя, тремя и четырьмя суперкадрами.

Табл. 1. Ил. 1.Библиогр.: 2 назв.

УДК 621.391.23

Особливості передачі даних по блоках у транкінгової системі стандарту APCO 25 / *І.В. Ковтун* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 270 – 274.

Розглянуто порівняльна характеристика основних перспективних стандартів цифрового транкінгового зв'язку TETRA, APCO 25 і TETRAPOL за експлуатаційно-технічним та організаційно-економічним критеріям. Проведено оцінку обсягу передачі даних по блоках у стандарті APCO 25. Розраховано час передачі даних для блоків з двома, трьома і чотирма суперкадрами.

Табл. 1. Іл. 1.Бібліогр.: 2 назви.

UDC 621.391.23

Especially data on blocks in the trunking system standard APCO 25 / *I.V. Kovtun* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 270 – 274.

The comparative characteristics of the main perspective standards of the digital trunked communication TETRA, APCO 25 and TETRAPOL by the operational-technical and organizational-economic criteria are considered. The evaluation of the data transmission volume to the blocks in the APCO 25 standard is carried out. Time of data transmission to the blocks with two, three and four super-frames is calculated.

1 tab. 1 fig. Ref.: 2 items.

УДК 621.391.001

Помехоустойчивость m-позиционного автокорреляционного приемника шумовых сигналов в гауссовом канале / *Ю.Г.Лега* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 275 – 282.

Представлены результаты теоретического исследования помехоустойчивости m-позиционного автокорреляционного приемника шумовых сигналов в канале с аддитивным белым гауссовым шумом.

Ил. 4. Библиогр.: 3 назв.

УДК 621.391.001

Завадостійкість m-позиційного автокореляційного приймача шумових сигналів в гауссовому каналі / *Ю.Г.Лега* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 275 – 282.

Представлено результати теоретичного дослідження завадостійкості m-позиційного автокореляційного приймача шумових сигналів в каналі з адитивним білим гауссовим шумом.

Іл. 4. Бібліогр.: 3 назв.

UDC 621.391.001

Noise-immunity of m-positional autocorrelation receiver of noise signals in the Gaussian channel / *Yu. G. Lega* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 275 – 282.

The results of theoretical researches of noise-immunity m-positional autocorrelation receiver of noise signals in the channel with additive white Gaussian noise are presented.

4 fig. Ref.: 3 items.

УДК 621.397.7

Особенности межкадрового сжатия видеоинформации в устройствах видеонаблюдения и видеорегистрации / *С.А.Шейко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 283 – 289.

Выявляются и анализируются причины появления «ложных» векторов движения при сжатии видеоизображений в системах видеонаблюдения и видеорегистрации. Показано, что использование оценочных функций, учитывающих битовые затраты на передачу векторов движения, позволяет избежать появления векторов при отсутствии движения, а также сократить скорость цифрового потока в системах видеонаблюдения до 10% в зависимости от степени сжатия. Также показана эффективность применения иерархического метода поиска векторов движения в видеопоследовательностях при малых отношениях сигнал-шум.

Ил. 5. Библиогр.: 8 назв.

УДК 621.397.7

Особливості міжкадрового стиснення відеоінформації в пристроях відеоспостереження та відеореєстрації / *С.О. Шейко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 283 – 289.

Виявляються та аналізуються причини виникнення «помилкових» векторів руху при стисненні відеозображень у системах відеоспостереження та відеореєстрації. Показано, що використання оціночних функцій, які враховують бітові витрати на передачу векторів руху, дозволяє уникнути появи векторів при відсутності руху, а також скоротити швидкість цифрового потоку в системах відеоспостереження до 10% залежно від ступеня стиснення. Також показано ефективність застосування ієрархічного методу пошуку векторів руху у відеопослідовностях при малих відношеннях сигнал-шум.

Іл. 5. Бібліогр.: 8 назв.

UDC 621.397.7

Particularities of inter frame coding of video information in the video monitoring and video recording devices / *S. O. Sheiko* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 283 – 289.

Reasons for “false” motion vectors appearance in the process of inter frame video coding in video monitoring and video recording devices are revealed and analyzed. It is shown that the use of the estimators taking into account the bit expenditures for the motion vectors transmission makes it possible to avoid appearance of vectors and to reduce digital flow velocity in the video observation systems up to 10% depending on the compression ratio. The efficiency of the hierarchical method for the motion vectors search in the video succession in the case of small SNR is also shown.

5 fig. Ref.: 8 items.

УДК 681.326

Методы планирования ресурсов в распределенных компьютерных системах / *В.Г. Котух, М.А. Мирошник, С.Н. Селевко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 290 – 299.

Предложен подход и модель планирования вычислительных ресурсов в двухуровневой *GRID*-системе. Разработана динамическая процедура планирования распределения ресурсов в гетерогенной среде на основе решения задачи о наименьшем покрытии. Разработан программный продукт, реализующий имитационную дискретно-событийную модель планирования. Проведены вычислительные эксперименты на основе программной реализации модели, обосновывающие эффективность предложенной модели планирования распределением ресурсов в гетерогенных средах в выбранных метриках производительности работы системы. Показано, что предложенная процедура планирования позволяет существенно повысить равномерность загрузки гетерогенных ресурсов системы, уменьшить время выполнения всей очереди заданий в *GRID*-системе по сравнению с распространенным методом *FIFO*. Приведен вариант реализации предложенного метода в планировщике *MAUI*

Ил. 2. Библиогр.: 8 назв.

УДК 681.326

Методи планування ресурсів в розподілених комп’ютерних / *В.Г. Котух, М.А. Мірошник, С.М. Селевко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 290 – 299.

Предложен подход и модель планирования вычислительных ресурсов в двухуровневой *GRID*-системе. Разработана динамическая процедура планирования распределения ресурсов в гетерогенной среде на основе решения задачи о наименьшем покрытии. Разработан программный продукт, реализующий имитационную дискретно-событийную модель планирования. Проведены вычислительные эксперименты на основе программной реализации модели, обосновывающие эффективность предложенной модели планирования распределением ресурсов в гетерогенных средах в выбранных метриках производительности работы системы. Показано, что предложенная процедура планирования позволяет существенно повысить равномерность загрузки гетерогенных ресурсов системы, уменьшить время выполнения всей очереди заданий в *GRID*-системе по сравнению с распространенным методом *FIFO*. Приведен вариант реализации предложенного метода в планировщике *MAUI*

Іл. 2. Бібліогр.: 8 назв.

UDC 681.326

Methods of resources planning in the distributed computer systems / *V.G. Kotuh, M.A. Miroshnik, S.N. Selevko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 290 – 299.

The approach and model of scheduling of computing resources in two-level *GRID* is offered. Dynamic procedure of scheduling resources in the heterogeneous environment on the basis of the decision of a problem on the minimal cover is developed. The software product realizing the imitating discrete-event model of

scheduling is developed. Computing experiments on the basis of the models program realization proving efficiency of the offered model of scheduling resources in heterogeneous environments in chosen metrics of performance of work of system are carried out. It is shown that the offered procedure of planning allows raising essentially the uniformity of loading of the system heterogeneous resources, reducing the performance time for tasks in *GRID*-system in comparison with the widespread combined method on the basis of *FCFS* method.

2 fig. Ref.: 8 items.

РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА
RADIO ENGINEERING DEVICES

УДК 621.372.852

Прямой метод синтеза полосно-пропускающих шлейфовых фильтров с чебышевской характеристикой / *Л.М. Карпуков, Р.Ю. Корольков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 300 – 305.

Предложен метод синтеза полосно-пропускающих фильтров с симметричной структурой, составленной из четвертьволновых отрезков линий и короткозамкнутых шлейфов. Метод позволяет непосредственно по техническому заданию без использования фильтров-прототипов составлять функцию фильтрации, обеспечивающую равноволновую амплитудную характеристику фильтра, и определять волновые сопротивления элементов фильтра с помощью простой процедуры, основанной на перемножении матриц. Приведен пример синтеза фильтра, показывающий, что по предложенному методу в отличие от традиционного метода на основе фильтра-прототипа, получается строго равноволновая характеристика фильтра при значениях волновых сопротивлений его элементов в большей мере удовлетворяющих требованиям конструктивной реализации.

УДК 621.372.852

Прямий метод синтезу смуго-пропускаючих шлейфових фільтрів з чебишевською характеристикою / *Л.М. Карпуков, Р.Ю. Корольков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 300 – 305.

Запропоновано метод синтезу смуго-пропускаючих фільтрів із симетричною структурою, складеної з чвертьхвильових відрізків ліній і короткозамкнутих шлейфів. Метод дозволяє безпосередньо за технічним завданням без використання фільтрів-прототипів складати функцію фільтрації, що забезпечує рівнохвильову амплітудну характеристику фільтра, і визначати хвильові опори елементів фільтра за допомогою простої процедури, яка заснована на перемножуванні матриць. Наведено приклад синтезу фільтра, який показує, що за запропонованим методом на відміну від традиційного методу на основі фільтра-прототипу, виходить строго рівнохвильова характеристика фільтра при значеннях хвильових опорів його елементів, що в більшій мірі задовольняють вимогам конструктивної реалізації.

UDC 621.372.852

Direct method for synthesis of bandpass stub filters with Chebyshev characteristic / *L.M. Karpukov, R.Y. Korolkov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 300 – 305.

The method for synthesis of bandpass filters with a symmetric structure, made of the quarter-wave segments of lines and short circuited stubs is offer. This method allows to make the function of filtration, providing equal to the wave peak characteristic of filter, and to determine the impendences of filter members by means of simple procedure, based on multiplying of matrices directly on a requirement specification without the use of filters-prototypes. The filter synthesis example is cited, showing, that according to the offered method, unlike the traditional method based on the filter-prototype, the filter strictly equal to the wave characteristic with the values of its elements impedances conforming to the needs of the structural realization is obtained.

УДК 621.372(075)

Схемы замещения конденсаторов и катушек индуктивности / *П.Ф.Лебедев, В.П.Дробышев* // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 306 – 312.

Рассмотрены три варианта методик преобразования RL- и RC-цепей на базовой частоте. Показано, что двухэлементные цепи катушек индуктивности и конденсаторов могут быть эквивалентно представлены двумя схемами замещения в частотной области, в которой допустимо такое представление. При этом возможны два подхода к анализу: либо эквивалентность осуществляют по входному

сопротивлению, либо по входной проводимости. Для катушек индуктивности более логичен первый вариант, для конденсаторов – второй.

Ил.4. Библиогр. 3 назв.

УДК 621.372(075)

Схеми заміщення конденсаторів та котушок індуктивності / *П.Ф. Лебедев, В.П. Дробышев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 306 – 312.

Розглянуто три варіанти методик перетворення RL- и RC-кіл на базовій частоті.Показано, що двоелементні кола котушок індуктивності та конденсаторів можуть бути еквівалентно представлені двома схемами заміщення в частотній галузі, в якій допустиме таке представлення. При цьому можливі два підходи до аналізу: або еквівалентність здійснюють за вхідним опором,або за вхідною провідністю. Для котушок індуктивності більш логічним є першій варіант, а для конденсаторів – другий.

Іл. 4. Бібліогр. 3 назв.

UDC 621.372(075)

Equivalent circuits of condensers and inductance coils / *P.F. Lebedev, V.P. Drobyshev* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 306 – 312.

Three versions of techniques for transformation of RL – and RC – circuits on the base frequency are considered. It is shown, that two-element circuits of inductance coils and condensers can be equivalently presented by two equivalent circuits in the frequency area where such representation is admissible. Thus two approaches to the analysis are possible: either the equivalence is realized on the entrance resistance, or on the entrance conductivity. The first version is more logical for the inductance coils, the second version is more logical for the condensers.

4 fig. Ref.: 3 items.

УДК 621.396.677.71

Анализ энергетических характеристик поперечной щели в широкой стенке прямоугольного волновода с локальным диэлектрическим включением / *Д.Ю. Пенкин, Л.П. Яцук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 313 – 321.

Численно исследованы диапазонные характеристики поперечной щели, прорезанной в широкой стенке прямоугольного волновода над локальным диэлектрическим включением, при различных геометрических параметрах структуры и значениях диэлектрической проницаемости вставки. Выявлены условия получения её коэффициента излучения близкого к единице, что, согласно теории волноводно-щелевых излучателей, недостижимо в случае однородного заполнения волновода. Показана возможность управления в широких пределах величинами энергетических параметров волноводно-щелевого элемента как при излучении в свободное полупространство, так и в другой прямоугольный волновод.

Ил. 6. Библиогр.: 4 назв.

УДК 621.396.677.71

Аналіз енергетичних характеристик поперечної щілини у широкій стінці прямокутного хвилеводу із локальним діелектричним вставленням / *Д.Ю. Пенкін, Л.П. Яцук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 313 – 321.

Чисельно досліджені діапазонні характеристики поперечної щілини, що прорізана у широкій стінці прямокутного хвилеводу над локальним діелектричним вставленням, за умови різних геометричних параметрів структури та значеннях діелектричної проникності вставки. Визначено умови отримання її коефіцієнта випромінювання близького до одиниці, що, згідно теорії хвилеводно-щілинних випромінювачів, недосяжно у разі однорідного заповнення хвилеводу. Показано можливість управління у широких межах величинами енергетичних параметрів хвилеводно-щілинного елементу як при випромінюванні у вільний напівпростір, так і в інший прямокутний хвилевід.

Іл. 6. Бібліогр.: 4 назв.

UDC 621.396.677.71

Analysis of power characteristics of the transversal slot in a wide wall of the rectangular waveguide with a local dielectric insertion / *D.Yu. Penkin, L.P. Yatsuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 313 – 321.

Scattering parameters of a cross slot, cut in a broadside of rectangular waveguide and located over a dielectric insertion of a finite length, are numerically investigated as functions of dimensions of waveguide-slot radiator and a dielectric constant of slab. The conditions, under which the radiation coefficient tends to be unity, are determined (note that such a result is unachievable for a waveguide with homogeneous inner configuration according to fundamentals of waveguide-slot radiator theory). An ability to control widely the

scattering parameters of waveguide-slot radiator, which emits either in free space or to another rectangular waveguide structure, is demonstrated.

6 fig. Ref.: 4 items.

УДК 621.372.832

Излучение электромагнитных волн электрически длинной щелью с диэлектрическим заполнением в узкой стенке многомодового прямоугольного волновода / *С. Л. Бердник* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. –.С. 322 – 326.

Методом Галеркина решена задача об излучении электромагнитных волн электрически длинной щелью с диэлектрическим заполнением в узкой стенке прямоугольного волновода, возбуждаемого высшими типами волн. Показана возможность реализации многочастотного излучателя на основе такой структуры при возбуждении волновода несколькими типами волн на разных частотах.

Ил. 4. Библиогр.: 6 назв.

УДК 621.372.832

Випромінювання електромагнітних хвиль електрично довгою щілиною з діелектричним заповненням у вузькій стінці багатомодового прямокутного хвилеводу / *С. Л. Бердник* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 322 – 326.

Методом Гальоркіна розв'язано задачу про випромінювання електромагнітних хвиль електрично довгою щілиною з діелектричним заповненням у вузькій стінці прямокутного хвилеводу, збуджуваного вищими типами хвиль. Показано можливість реалізації багаточастотного випромінювача на основі такої структури при збудженні хвилеводу декількома типами хвиль на різних частотах.

Іл. 4. Бібліогр.: 6 назв.

UDC 621.372.832

Radiation of electromagnetic waves by electrically long slot with dielectric filling in the narrow wall of the multimode rectangular waveguide / *S. L. Berdnik* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 322 – 326.

The problem of the radiation of electromagnetic waves by electrically long slot with dielectric filling in the narrow wall of rectangular waveguide excited by higher types of waves have been solved by the Galerkin's method. It is shown that the multi-frequency radiator based on this structure has been realized in the case of excitation of the waveguide by several modes.

4 fig. Ref.: 6 items.

УДК 681.7.068.4

Моделирование влияния структуры фотонно-кристаллических волокон на распределение модового поля и потери оптического сигнала в их соединениях / *А.И. Филипенко, О.В. Сычова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 327 – 331.

Исследованы факторы потерь в соединениях между собой и с SMF волокнами нескольких моделей ФКВ с разной структурой поперечного сечения, путем моделирования получены их распределения поля основной моды, количественно оценено и проанализировано влияние оптико-геометрических отклонений, возникающих при соединении, на оптические потери.

Табл. 2. Ил. 6. Библиогр.: 5 назв.

УДК 681.7.068.4

Моделювання впливу структури фотонно-кристалічних волокон на розподіл модового поля та втрати оптичного сигналу в їх з'єднаннях / *О.І. Филипенко, О.В. Сичова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 327 – 331.

Досліджено фактори втрат у з'єднаннях між собою й з SMF волокнами декількох моделей ФКВ із різною структурою поперечного перерізу, шляхом моделювання отримані їхні розподіли поля основної моди, кількісно оцінене й проаналізоване вплив оптико-геометричних відхилень, що виникають при з'єднанні, на оптичні втрати.

Табл. 2. Іл. 6. Бібліогр.: 5 назв.

UDC 681.7.068.4

Modeling of the photonic crystal fiber structure impact on the mode field distribution and on the optical signal loss in their connections / *A. I. Filipenko, O.V. Sychova* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 327 – 331.

Loss factors in connections among themselves and with SMFs of several models PCFs with different structure of cross-section are researched, distributions of a basic mode field PCFs are received by modeling

and impact of the optic-geometrical deviations arising at connection on optical losses is quantitatively estimated and analyzed.

2 tab. 6 fig. Ref.: 5 items.

УДК 621.315.592

Исследование и оптимизация пленочных кремниевых аморфных фотопреобразователей на *p-i-n*-структурах / *Н.И. Слипченко, В.А. Письменецкий, А.В. Фролов, Н.В. Герасименко, М.Ю. Гуртовой, Е.С. Глушко, Т.Е. Стыценко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2012. – Вып. №171. – С. 332 – 339.

Исследованы и оптимизированы параметры тандемной пленочной кремниевой *p-i-n* гетероструктуры. Проведены расчеты *p-i-n* ячеек и экспериментальные исследования подсистемы солнечной станции, состоящей из панелей на основе аморфного кремния, которые подтвердили целесообразность их оптимизации.

Ил. 12. Библиогр.: 5 назв.

УДК 621.315.592

Дослідження і оптимізація плівкових кремнієвих аморфних фотоперетворювачів на *p-i-n*-структурах / *М.І. Сліпченко, В.О. Письменецький, А.В.Фролов, М.В. Герасименко, М.Ю. Гуртовий, О.С. Глушко, Т.Є. Стиценко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. № 171. – С. 332 – 339.

Досліджено і оптимізовано параметри тандемної плівкової кремнієвої *p-i-n* гетероструктури. Проведено розрахунки *p-i-n* комірок та експериментальні дослідження підсистеми сонячної станції, що складається з панелей на основі аморфного кремнію, які підтвердили доцільність їх оптимізації.

Іл. 12. Бібліогр.: 5 назв.

UDC 621.315.592

Research and optimization of p-i-n structures based on the amorphous silicon films / *N.I. Slipchenko, V.A. Pismenetskiy, A.V. Frolov, N.V. Gerasimenko, M.Y. Gurtovoy, L.G. Glushko, T.E. Stytsenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. – N171. – P. 332 – 339.

Parameters for tandem p-i-n heterostructure consisting of silicon films were investigated and optimized. The calculations of p-i-n cells and experimental studies of the solar sub station consisting of panels based on the amorphous silicon confirmed the feasibility of their optimization.

12 fig. Ref.: 5 items.

УДК 528::629.783

Разработка и тестирование новых эффективных методов и алгоритмов обнаружения и устранения фазовых скачков статических и кинематических ГНСС–наблюдений / *А.А. Жалило.* // Радиотехника : Всеукр. межвед. науч.-техн. сборник. – 2012. – Вып. 171. С. 340 - 371.

Рассматривается задача определения потерь счета циклов в одночастотных и двухчастотных фазовых ГНСС–наблюдениях и их исправления. Описаны результаты разработки и тестирования новых эффективных методов и алгоритмов обнаружения, оценки и исправления фазовых скачков как статических, так и кинематических ГНСС–наблюдений. Рассмотрены два отличающихся метода обработки наблюдений. Первый из них реализует интервальную итерационную процедуру обнаружения и оценки (фиксации) скачков одинарных разностей фаз между парами спутников с последующей их идентификацией на отдельных трассах «спутники – приемник». Расширить возможности и повысить надежность устранения фазовых скачков одночастотных и двухчастотных кинематических наблюдений в сложных условиях (разрывы и пропуски наблюдений) позволяет применение другого предложенного метода. Он основан на использовании приращений наблюдений по времени и специальной процедуры совместного МНК–оценивания совокупности континуальных (приращений координат и расхождений часов) и дискретных параметров (циклических фазовых скачков).

Табл. 1. Ил. 4 Библиогр.: 16 назв.

УДК 528::629.783

Розробка і тестування нових ефективних методів і алгоритмів виявлення та усунення фазових стрибків статичних і кінематичних ГНСС–спостережень / О.О. Жаліло // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2012. – Вип. 171. С. 340 - 371.

Розглядається задача визначення втрат рахунку циклів в одночастотних і двочастотних фазових ГНСС–спостереженнях та їх виправлення. Описані результати розробки і тестування нових ефективних методів і алгоритмів виявлення, оцінки і виправлення фазових стрибків як статичних, так і кіне-

матичних ГНСС–спостережень. Розглянуто два методи обробки спостережень, що відрізняються. Перший з них реалізує інтервальну ітераційну процедуру виявлення і оцінки (фіксації) стрибків одинарних різниць фаз між парами супутників з наступною їх ідентифікацією на окремих трасах «супутники – приймач». Розширити можливості і підвищити надійність усунення фазових стрибків одночастотних і двочастотних кінематичних спостережень в складних умовах (розриви і пропуски спостережень) дозволяє застосування іншого запропонованого методу. Він заснований на використанні прирощень спостережень за часом і спеціальної процедури спільного МНК–оцінювання сукупності континуальних (прирощень координат і розбіжностей годинників) і дискретних параметрів (циклічних фазових стрибків).

Табл.1. Іл. 4 . Бібліогр.: 16 назв.

UDC УДК 528::629.783

Development and testing of new methods and algorithms for detecting and correction the carrier-phase slips of static and kinematic GNSS observations / A.A.Zhalilo // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2012. № 171. – P. 340 - 371.

The task of determining cycle counting losses in single- and dual-frequency carrier-phase GNSS observations and their repair is studied. It is described the results of development and testing of new effective methods and algorithms for detection, assessment and repair of carrier-phase jumps (slips) of both static and kinematic GNSS observations. Two different methods of observation processing are considered. The first one implements interval iterative detection procedure and estimation (fixing) of slips of carrier-phase single differences between pairs of satellites with their subsequent identification on separate tracks «satellites–receiver». Using of other method enables to enhance possibilities and increase reliability of eliminating the carrier-phase slips of single- and dual-frequency kinematic observations in difficult circumstances (gaps and missing observations). It is based on using the increments of observations by time and special procedure for joint LSM–estimation of combining the continuum (increments of coordinates and clock variations) and discrete parameters (carrier-phase cycle slips).

1 Tab. 4 Fig. Ref.: 16 items.