СИНТЕЗ И АНАЛИЗ СИММЕТРИЧНЫХ КРИПТОПРИМИТИВОВ
SYNTHESIS AND ANALYSIS OF SYMMETRIC CRYPTOPRIMITIVES

УДК 681.3.06

Моделирование атак на отказ в обслуживании для web-приложений с применением бот-сетей / *Р.В. Олейников, Д.В. Мурин, С.В. Килипко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 7 – 12.

Предложен метод предсказания увеличения нагрузки на web-приложение и расчета эффективности компьютерной системы в заданный период времени в условиях возможности реализации атаки на отказ в обслуживании. Разработана модель атак на отказ в обслуживании, вызванная самораспространяющимися агентами вредоносного ПО, объединенными в бот-сеть. Приведен численный анализ эффективности защиты систем с применением антивирусного программного обеспечения.

Ил. 10. Библиогр.: 4 назв.

УДК 681.3.06

Моделювання атак на відмову в обслуговуванні для web-додатків із застосуванням бот-мереж / *Р.В. Олійников, Д.В. Мурін, С.В. Килипко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 7 – 12.

Запропоновано метод прогнозування збільшення навантаження на web-додатки і розрахунку ефективності комп'ютерної системи за вказаний період часу в умовах можливих атаки на відмову в обслуговуванні. Розроблена модель атак на відмову в обслуговуванні, що викликані агентами зловмисного програмного забезпечення, що само розповсюджується, та які об'єднані в бот-мережу. Наведений чисельний аналіз ефективності систем захисту із застосуванням антивірусного програмного забезпечення.

Іл. 10. Бібліогр.: 4 назв.

UDC 681.3.06

Modelling of botnet based DDoS attacks targeted to web applications / *R.V. Oliynykov, D.V. Murin, S.V. Kylypko* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 7 – 12.

A method for prediction of web application load increase and calculate system efficiency during given period of time with condition of Denial-of-Service attack possibility is proposed. A model of DDoS attacks caused by malicious self-speading software agents united into botnet is developed. Numeric analysis of system protection with application of antivirus (antimalware) solutions is considered.

10 fig. Ref.: 4 items.

УДК 621.391:519.2

Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / *А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 13 – 20.

Предложена атака на генератор гаммы с линейным законом реинициализации начального состояния, которую можно использовать при менее жестких ограничениях относительно функции усложнения генератора по сравнению с аналогичными ранее известными атаками.

Табл. 3. Ил.1. Библиогр.: 8 назв..

УДК 621.391:519.2

Статистична атака на генератор гами з лінійним законом реініціалізації початкового стану та функцією ускладнення, що є близькою до алгебраїчно виродженої / *А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 13 – 20.

Запропоновано атаку на генератор гами з лінійним законом реініціалізації початкового стану, яка є застосовною за менш жорстких обмежень відносно функції ускладнення генератора у порівнянні з аналогічними раніше відомими атаками.

Табл. 3. Іл. 1. Бібліогр.: 8 назв.

UDC 621.391:519.95

Statistical attack on key-stream generator with linear re-initialization mechanism and output function close to an algebraic degenerate one / *A.N. Alekseychuk, S.N. Konushok, A.Y. Storozhuk //* Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 13 – 20.

An attack on a key-stream generator with linear re-initialization mechanism is proposed. In contrast to similar previously known attacks, the proposed attack is applicable under less stringent conditions about the generator's function.

3 tab. 1 fig. Ref.: 8 items.

УДК 681.3.06

Построение нетривиальных кривых Гурвица / *О.Г. Халимов, Е.В. Алекси, Г.З. Халимов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 21 – 26.

Представлено решение задачи построения кривых Гурвица минимального рода по делителям порядка конечного поля на основе метода реализующего последовательный подъем от кривых с наименьшими показателями степеней к искомым, которые соответствуют заданному значению рода. Рассмотрены свойства переборного метода построения кривых Гурвица по делителям порядка конечного поля, примеры построения кривых по заданному роду. Показано, что предложенный метод расширяет множество кривых, так как определяет построение кривых по произвольному набору делителей порядка поля с временем вычисления степенных показателей кривой, которое не зависит от числа делителей.

Табл.: 1. Библиогр.: 7 назв.

УДК 681.3.06

Побудова нетривіальних кривих Гурвіца / *О.Г. Халімов, Є.В. Алекси, Г.З. Халімов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 21 – 26.

Представлено рішення задачі побудови кривих Гурвіца мінімального роду по дільникам порядку кінцевого поля на основі методу, що реалізує послідовний підйом від кривих з найменшими показниками ступенів до шуканих , які відповідають заданому значенню роду . Розглянуто властивості переборного методу побудови кривих Гурвіца по дільникам порядку кінцевого поля , приклади побудови кривих по заданому роду. Показано, що запропонований метод розширює безліч кривих, так як визначає побудову кривих по довільному набору дільників порядку поля з часом обчислення ступенів показників кривої , яке не залежить від числа дільників.

Табл. 1. Бібліогр.: 7 назв.

UDC 681.3.06

Nontrivial Hurwitz curves construction / *O.G. Khalimov, E.V. Alexi, G.Z. Khalimov* // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 21 – 26.

The solution is presented to the problem of constructing a minimal kind of Hurwitz curves over divisors of the order of a finite field, based on the method of implementing a consistent rise of the curves with the lowest degrees to the sought that match the specified value kind. The properties of exhaustive search method for constructing Hurwitz curves over divisors of the order of a finite field are considered, examples of construction of curves for a given age are cited. It is shown that the proposed method expands the set of curves , as it determines the construction of curves on an arbitrary set of divisors of the order of the field with the computation time exponents of the curve, which is independent of the number of divisors .

Tab.: 1. Refs.: 7 titles.

УДК 621. 3.06

О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным / *І.Д. Горбенко, К.Е. Лисицкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 27 – 39.

Предлагается новая методика определения числа циклов, необходимых для прихода шифров к состоянию случайной подстановки. Излагаются результаты применения этой методики для оценки динамических показателей перехода к показателям случайной подстановки ряда современных блочных симметричных шифров, в том числе шифров, представленных в свое время на украинский конкурс по выбору претендента на национальный стандарт блочного симметричного шифрования. Оценивается перспективность использования в шифрах случайных S-блоков.

Табл. 8 Билиогр. : 16 назв.

УДК 621. 3.06

Про динаміку приходу шифрів до випадкової підстановці при використанні S-блоків з показниками нелінійності близькими до граничних / *І.Д. Горбенко, К.Є. Лисицький* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 27 – 39.

Пропонується нова методика визначення числа циклів, необхідних для приходу шифрів до стану випадкової підстановки. Викладаються результати застосування цієї методики для оцінки динамічних показників переходу до показників випадкової підстановки ряду сучасних блокових симетричних шифрів, в тому числі шифрів, представлених в свій час на український конкурс з вибору претендента на національний стандарт блокового симетричного шифрування. Оцінюється перспективність використання в шифри випадкових S-блоків.

Табл. 8. Бібліогр. : 16 назв.

UDC 621. 3.06

The dynamics of the parish to a random permutation ciphers using S-boxes with exponents of nonlinearity close to the limit / *I.D. Gorbenko, K.E. Lisitskiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 27 – 39.

A new method for determining the number of cycles required for the arrival of a cipher as a random permutation. The results are presentedof applying this technique to assess the dynamic performance indicators of transition to a random permutation of a number of contemporary block symmetric ciphers, including ciphers submitted in due time on the Ukrainian competition to select a challenger for the national standard symmetric encryption block. The prospects of using Ranked random S-boxes in ciphers are estimated.

8 tab. Ref. 16 items

УДК 004.056.55

Статистические свойства блочных симметричных шифров международного стандарта ISO / IEC 29192-2 / *И.Д. Горбенко, А.А. Кузнецов , А.В. Самойлова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 40 – 44.

Рассматриваются алгоритмы блочного симметричного шифрования, определенные в международном стандарте ISO / IEC 29192-2. Это так называемые облегченные (Lightweight) шифры, предназначенные для использования в упрощенных приложениях, например, в смарт-картах. С использованием методики статистических исследований случайных и псевдослучайных последовательностей NIST STS проводится сравнительный анализ статистических свойств блочных симметричных шифров из стандартов ISO / IEC 29192-2, FIPS - 197 и ГОСТ 28147-89. Экспериментальные исследования проведены для случая применения пяти режимов шифрования (ECB, CBC, CFB, CTR и OFB), которые определены в международном стандарте ISO / IEC 10116-2006. Показано, что по показателям статистической безопасности шифры из ISO / IEC 29192-2 несколько уступают алгоритмам FIPS - 197 и ГОСТ 28147-89.

Табл. 2. Ил. 7. Библиогр.: 7 назв.

УДК 004.056.55

Статистичні властивості блокових симетричних шифрів з міжнародного стандарту ISO/IEC 29192-2 / *І.Д. Горбенко, О.О. Кузнецов, А.В. Самойлова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 40 – 44.

Розглядаються алгоритми блокового симетричного шифрування, які визначено в міжнародному стандарті ISO/IEC 29192-2. Це так звані облегшені (Lightweight) шифри, які призначено для використання в спрощених застосуваннях, наприклад, в смарт-картках. Із використанням методики статистичних досліджень випадкових та псевдовипадкових послідовностей NIST STS проводиться порівняльний аналіз статистичних властивостей блокових симетричних шифрів зі стандартів ISO/IEC 29192-2, FIPS-197 та ГОСТ 28147-89. Експериментальні дослідження проведено для випадку застосування п’яти режимів шифрування (ECB, CBC, CFB, CTR та OFB), які визначено в міжнародному стандарті ISO/IEC 10116-2006. Показано, що за показниками статистичної безпеки шифри з ISO/IEC 29192-2 дещо поступаються алгоритмам FIPS-197 та ГОСТ 28147-89.

Табл. 2. Іл. 7. Бібліогр.: 7 назв.

UDC 004.056.55

Statistical properties of symmetric block cipher of the ISO / IEC 29192-2 international standard. / *I.D. Gorbenko, O.O. Kuznetsov, A.V. Samoilova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 40 – 44.

The block ciphers defined in the ISO/IEC 29192-2 international standard are considered. These are so-

called facilitated (Lightweight) codes intended for using in the simplified applications, e.g, in smart cards. Using methods of statistical studies of random and pseudo-random sequences NIST STS conducted a comparative analysis of the statistical properties of symmetric block ciphers Standards ISO/IEC 29192-2, FIPS-197 and GOST 28147-89. Experimental studies have been carried out for the case of five modes of encryption (ECB, CBC, CFB, CTR and OFB), as defined in the international standard ISO / IEC 10116-2006. It is shown that the statistical indicators of security codes from ISO/IEC 29192-2 rank below FIPS- 197 algorithms and GOST 28147-89.

2 tab. 7 fig. Ref.: 7 items.

УДК 004.056.55

Исследование режимов применения блочных симметричных шифров в соответствии с ISO/IEC 10116-2006 // *А.А. Кузнецов, Р.И. Мордвинов, Е.П. Колованова, А.В. Самойлова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 45 – 54.

Исследуются режимы применения блочных симметричных шифров, которые определены в международном стандарте ISO/IEC 10116-2006. Анализируются особенности применения блочных симметричных шифров в различных режимах и исследуются их криптографические свойства по обеспечению определенных услуг безопасности. Проводятся статистические исследования последовательностей псевдослучайных битов, которые сформированы с использованием различных режимов шифрования, в частности исследуется статистическая безопасность шифров ГОСТ 28147-89, TDEA, FIPS-197, Camellia и Калина в режимах шифрования, определенных в ISO/IEC 10116-2006 .

Табл. 1. Ил. 8. Библиогр.: 9 назв.

УДК 004.056.55

Дослідження режимів застосування блокових симетричних шифрів відповідно до ISO/IEC 10116-2006 / *О.О. Кузнецов, Р.І. Мордвінов, Є.П. Колованова, А.В. Самойлова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 45 – 54.

Досліджуються режими застосування блокових симетричних шифрів, які визначені в міжнародному стандарті ISO/IEC 10116-2006. Аналізуються особливості застосування блокових симетричних шифрів у різних режимах та досліджуються їх криптографічні властивості із забезпечення певних послуг безпеки. Проводяться статистичні дослідження послідовностей псевдовипадкових бітів, які сформовані із використанням різних режимів шифрування, зокрема досліджується статистична безпека шифрів ГОСТ 28147-89, TDEA, FIPS-197, Camellia та Калина у режимах шифрування, визначених у ISO/IEC 10116-2006.

Табл. 1. Іл. 8. Бібліогр.: 9 назв.

UDC 004.056.55

Investigation into symmetric block cipher modes application in accordance with ISO/IEC 10116-2006 // *O.O. Kuznetsov, R.I. Mordvinov, E.P. Kolovanova, A.V. Samoilova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 45 – 54.

The modes of using the block symmetric ciphers defined in the international standard ISO/IEC 10116-2006 were investigated. The features use symmetric block ciphers in various modes and investigated their cryptographic properties to ensure certain security services. Statistical investigations were carried out into the sequences of pseudo-random bits generated using different encryption modes, including the statistical security of ciphers of GOST 28147-89, TDEA, FIPS-197, Camellia and Viburnum encryption modes defined in ISO/IEC 10116-2006.

1 tab. 8 fig. Ref.: 9 items.

УДК 004.056.55

Об условиях отсутствия эффективных усеченных байтовых дифференциалов для блочных симметричных шифров / *В.И. Руженцев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 55 – 61.

Внимание сосредотачивается на уточнении представленного в одной из предыдущих работ подхода к доказательству эффективных байтовых дифференциалов, которые могут быть положены в основу атаки на блочный шифр. Выполняется распространение представленного ранее для отдельного класса шифров подхода на блочные шифры в целом. Выделены достаточные для отсутствия эффективных байтовых дифференциалов условия.

Табл. 4. Ил. 1. Библиогр.: 8 назв.

УДК 004.056.55

Про умови відсутності ефективних усічених байтових диференціалів для блокових симетричних шифрів / *В.І. Руженцев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 55 – 61.

Увага приділяється уточненню представленого в одній з попередніх робіт підходу до доведення відсутності ефективних байтових диференціалів, що можуть бути покладені в основу атаки на блоковий шифр. Представлений раніше для окремого виду шифрів підхід розпространяється на блокові шифри взагалі. Виділені достатні умови відсутності ефективних байтових диференціалів.

Табл. 4. Іл. 1. Бібліогр.: 8 назв.

UDC 004.056.55

About conditions of effective truncated byte differential absence for block ciphers / *V.I. Ruzhentsev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 55 – 61.

The attention is paid to the correction of presented in the previous paper approach to proving the effective byte differentials absence. The presented in the previous paper approach were used for one type of block cipher. In this paper it spread on the block cipher in general. The sufficient conditions for effective byte differentials absence is selected.

4 tab. 1 fig. Ref.: 8 items.

СИНТЕЗ И АНАЛИЗ АСИММЕТРИЧНЫХ КРИПТОПРИМИТИВОВ
SYNTHESIS AND ANALYSIS OF ASYMMETRIC CRYPTOPRIMITIVES

УДК 004.032.26

Генератор псевдослучайных последовательностей на основе модифицированной рекуррентной нейронной сети / *Е. А. Винокурова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 62 – 67.

Генераторы псевдослучайных чисел являются неотъемлемым модулем криптографических систем. В статье предлагается генератор псевдослучайных последовательностей на основе модифицированной рекуррентной нейронной сети. Предложен метод обучения модифицированной рекуррентной нейронной сети. Результаты экспериментов подтверждают эффективность предложенного подхода.

Ил. 1. Библиогр.: 18 назв.

УДК 004.032.26

Генератор псевдовипадкових послідовностей на основі модифікованій рекурентній нейронній мережі / *Є. А. Винокурова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 62 – 67.

Генератори псевдовипадкових чисел є невід'ємним модулем криптографічних систем. Запропоновано генератор псевдовипадкових послідовностей на основі модифікованій рекурентній мережі. Запропоновано метод навчання модифікованій рекурентній нейронній мережі. Результати експериментів підтверджують ефективність запропонованого підходу.

Іл.1. Бібліогр.: 18 назв.

UDC 004.032.26

Pseudorandom number generator based on modified neural network / *O. A. Vynokurova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 62 – 67.

A pseudorandom number generators are inalienable module cryptographic systems. The pseudorandom number generator based on modified recurrent neural network is proposed. The learning algorithm of modified recurrent neural network is developed. Theoretical justification and experimental results prove the efficiency of the developed approach.

1 fig. Ref. : 18 items.

УДК 621.391:519.2:519.7

Оценка стойкости направленного шифра NTRU к атаке, основанной на изменениях времени расшифрования / *А.П. Бубырь, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 68 – 73.

Представлены результаты исследования возможности практической реализации атаки, основан-

ной на изменениях времени расшифрования в алгоритме направленного шифрования NTRU. Экспериментально определена зависимость вероятности успешной реализации атаки от используемых общесистемных параметров. Установлено, что наборы параметров, рекомендованные к использованию стандартом ANSI X9.98, не подвержены данной атаке, т.к. вероятность ее успешного проведения стремится к нулю.

Табл. 1. Библиогр.: 2 назв.

УДК 621.391:519.2:519.7

Оцінка стійкості направленого шифру NTRU до атаки, заснованої на змінах часу розшифрування / *А.П. Бубир, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 68 – 73.

Представлені результати дослідження можливості практичної релізації атаки, заснованої на змінах часу розшифрування в алгоритмі направленого шифрування NTRU. Експериментально визачена залежність ймовірності успішної реалізації атаки від використаних загальносистемних параметрів. Встановлено, що набори параметрів, які рекомендовані до використання стандартом ANSI X9.98, не вразливі до даної атаки, тому що ймовірність її успішного проведення наближається до нуля.

Табл 1. Бібліогр.: 2 назви.

UDC 621.391:519.2:519.7

Evaluation of lattice-based public key algorithm NTRU resistance against timing attack / *A.P. Bubyr, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 68 – 73.

Results of research in timing attack against asymmetric cipher NTRU are given. Dependence of probability of successful attack execution on the used system-wide parameters was defined experimentally. It was found that parameter sets from standard ANSI X9.98 are not vulnerable.

1 tabl. Ref.: 2 items.

УДК 519.713

Анализ условий имплементации электронной идентификации и доверительных услуг для электронных операций на внутреннем рынке / *А. А. Бойко, Ю. А. Сергийчук, А. В. Триполка* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 74 – 87.

Представлены результаты анализа возможности имплементации электронной идентификации и доверительных услуг для электронных операций на внутреннем рынке согласно требованиям проекта Регламента Европейского парламента и Совета. Даны рекомендации относительно политик использования протоколов SSL / TLS для аутентификации веб-сайтов.

Ил. 10. Библиогр.: 31 назв.

УДК 519.713

Аналіз умов імплементації електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку / *А. О. Бойко, Ю. О. Сергійчук, А. В. Трипілка* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 74 – 87.

Представлено результати аналізу можливості імплементації електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку згідно вимогам проекту Регламенту Європейського парламенту і Ради. Надані рекомендації щодо політик використання протоколів SSL/TLS для автентифікації веб-сайтів.

Іл. 10. Бібліогр.: 31 найм.

UDC 519.713

Analysis of conditions for implementation of electronic identification and trusted services for electronic transactions in the domestic market / *A. Boiko, Y. Sergiichuk, A. Trypilka* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – №N 176. – P. 74 – 87.

The paper presents an analysis of the possibilities to implement the electronic identification and trusted services for electronic transactions in the domestic market to meet the requirements of the project of the European Parliament and the Council. Recommendations for the policy of SSL / TLS protocols usage in the authenticate websites.

Fig. 10. Ref.: 31 items.

УДК 681.3.06

Изоморфизм несуперсингулярных кривых над полями характеристики 2 и кривых Эдвардса с одним параметром / *А.В. Бессалов, А.А. Дихтенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 88 – 92.

Рассмотрены аффинное и проективное представления эллиптической кривой в форме Эдвардса

над полями F_2^m. Даны оценки сложности выполнения групповых операций в проективных координатах. Получены условия существования несуперсингулярной кривой, изоморфной кривой Эдвардса с одним параметром *d*. Для известных стандартных кривых, удовлетворяющих этим условиям, найдены изоморфные им кривые Эдвардса.

Табл. 2. Библиогр.: 9 назв.

УДК 681.3.06

Ізоморфізм несуперсингулярних кривих над полями характеристики 2 та кривих Едвардса з одним параметром / *А.В. Бессалов, А.А. Діхтенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 88 – 92.

Розглянуто афінне та проективне представлення еліптичної кривої в формі Едвардса над полями F_2^m. Дані оцінки складності виконання групових операцій в проективних координатах. Отримані умови існування несуперсингулярної кривої, що ізоморфна кривій Едвардса з одним параметром *d*. Для відомих стандартних кривих, що задовольняють цим умовам, знайдені ізоморфні криві Едвардса.

Табл. 2. Бібліогр.: 9 назв.

UDC 681.3.06

Birational equivalence between canonical elliptic curves over fields of characteristics 2 and Edwards curves / *A.V. Bessalov, A.A. Dihtenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 88 – 92.

The affine and projective representations are considered for the Edwards curve over fields F_2^m. Evaluations are given for the group operations complexity in the projective coordinates. The conditions are obtained for the canonical curve which is isomorphic to the Edwards curve with one parameter *d*. The isomorphic Edwards curves are found for the of known standard curves, which satisfy these conditions.

2 tab. Ref.: 9 items.

УДК 004.056.55

Кодирование информации точками на эллиптической кривой / *С.С. Тимохин, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 93 – 96.

Эллиптические кривые имеют наибольшую устойчивость среди существующих методов асимметричной криптографии. Но они почти не используются для поточного шифрования из-за сложности представления точки на эллиптической кривой. Рассматриваются существующие методы представления информации в виде точки на эллиптической кривой.

Библиогр.: 3 назв.

УДК 004.056.55

Кодування інформації точками на еліптичній кривій / *С.С. Тімохін, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 93 – 96.

Еліптичні криві мають найбільшу стійкість серед існуючих методів асиметричної криптографії. Але вони майже не використовуються для поточного шифрування через складність представлення точки на еліптичній кривій. У цій статті розглядаються існуючі методи представлення інформації у вигляді точки на еліптичній кривій.

Бібліогр.: 3 назв.

UDC 004.056.55

Encoding of information using points on elliptic curves / *S.S. Timohin, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 93 – 96.

Elliptic curves have the greatest resistance of existingasymmetric cryptography methods. But they are almost never used for encryption because of complexity of representing the points on an elliptic curve. This article discusses existing methods of presenting information in the form of points on the elliptic curve.

Ref.: 3 items.

МЕХАНИЗМЫ И СРЕДСТВА ЗАЩИТЫ СЕТЕЙ СВЯЗИ
MECHANISMS AND MEANS OF COMMUNICATION NETWORK PROTECTION

УДК 004.056.57

Статистический анализ сетевого трафика для систем обнаружения и предотвращения вторжений / *А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко, А. Березовский* // Радиотехника : Всеукр.

межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 97 – 110.

Рассматриваются системы обнаружения и предотвращения вторжений, функционирование которых базируется на исследовании аномалий сетевого трафика (Anomaly-BasedIntrusionDetectionand PreventionSystems). Проводится статистический анализ временных рядов, характеризующих сетевой трафик различных служб и информационных сервисов современных телекоммуникационных систем и сетей. Исследуется однородность сетевого трафика по различным критериям, показано, что применение методов статистического анализа позволяет успешно проводить мониторинг сетевой активности для обнаружения вторжений и предотвращения их воздействия на защищаемые информационные ресурсы.

Табл. 5. Ил. 10. Библиогр.: 17 назв.

УДК 004.056.57

Статистичний аналіз мережевого трафіку для систем виявлення та запобігання вторгнень / *О.О. Кузнецов, Р.І., А.А. Смірнов, Д.А. Даниленко, А. Березовський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 97 – 110.

Розглядаються системи виявлення та запобігання вторгнень, функціонування яких базується на дослідженні аномалій мережевого трафіку (Anomaly – BasedIntrusionDetectionandPreventionSystems). Проводиться статистичний аналіз часових рядів, що характеризують мережевий трафік різних служб та інформаційних сервісів сучасних телекомунікаційних систем і мереж. Досліджується однорідність мережевого трафіку за різними критеріями, показано, що застосування методів статистичного аналізу дозволяє успішно проводити моніторинг мережевої активності для виявлення вторгнень і запобігання їх впливу на захищаються інформаційні ресурси .

Табл. 5. Іл. 10. Бібліогр.: 17 назв.

UDC 004.056.57

Statistical analysis of network traffic detection systems and intrusion prevention // *O.O. Kuznetsov, A.A. Smirnov, D.A. Danilenko, A. Berezovskiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 97 – 110.

The systems of intrusion detection and prevention are considered, the operation of which is based on the study of network traffic anomalies (Anomaly-BasedIntrusionDetectionandPreventionSystems). Statistical analysis of time series describing the network traffic of various services and information services of modern telecommunication systems and networks is carried out. The homogeneity of network traffic according to various criteria is investigated, it is shown that the use of statistical analysis makes it possible to monitor the network activity successfully for intrusion detection and prevention of their impact on the protected information resources.

5 tab. 10 fig. Ref.: 17 items.

УДК 004.75:004.05

Механизмы защищенного обмена данными в облачных вычислениях / *И.Д. Горбенко, М.И. Харламб* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 111 – 115.

Рассматривается общая структура построения системы облачных вичислений, возможные угрозы в системе. Определяется актуальность использования механизмов защищенного обмена данными. Проводится анализ и предлагается использование криптосистемы ECIES.

Ил.3. Библиогр.: 5 назв.

УДК 004.75:004.05

Механізми захищеного обміну інформацією при обчисленнях в хмарі / *І.Д.Горбенко, М.І.Харламб* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 111 – 115.

Розглядається загальна побудова системи хмарних обчислень, можливі загрози в системі. Визначається актуальність використання механізмів захищеного обміну даними. Проводиться аналіз та пропонується використання криптосистеми ECIES.

Іл.3. Бібліогр.: 5 назв.

UDC 004.75:004.05

Mechanisms for secure communication in cloud computing / *I.D. Gorbenko, M.I. Kharlamb* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 111 – 115.

The general structure of building a system of cloud computing, possible threats to the system are considered. The relevance of secure communication mechanisms is estimated. Analyzes and proposes as to the use of ECIES cryptosystem are offered.

3 fig., Ref.:5items.

УДК 004.56:004.353.2

Исследования изменения формы сигнала в канале побочных электромагнитных излучений монитора / *В.И. Заболотный, Е.В. Герасименко, В.И. Перепадя* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 116 – 121.

На основе анализа решений Максвелла, показана смена формы отклика наведенных значений э.д.с. в антенне разведывательного устройства в дальней зоне канала ПЕМИ. Установлено, что форма э.д.с. для электрической антенны соответствует второй производной исходного сигнала, а для магнитной - третий. Используя свойства преобразований Фурье, определены спектральные функции разведанных сигналов. Показана возможность определения величин параметров исходных сигналов по значениям измеренных «нулей» спектра ПЕМИ.

Ил. 4. Библиогр.: 4 назв.

УДК 004.56:004.353.2

Дослідження зміни форми сигналу у каналі побічних електромагнітних випромінювань монітору / *В.І. Заболотний, Є.В. Герасименко, В.І. Перепадя* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 116 – 121.

На основі аналізу рішень Максвела, показана зміна форми відгуку наведених значень е.р.с. у антені розвідувального пристрою у дальній зоні каналу ПЕМВ. Встановлено, що форма е.р.с. для електричної антени відповідає другій похідній вихідного сигналу, а для магнітної – третій. Використовуючи властивості Фур'є перетворювань, визначено спектральні функції розвідуваних сигналів. Показано на можливість визначення величин параметрів вихідних сигналів по значенням виміряних «нулів» спектру ПЕМВ.

Ил. 4. Бібліогр.: 4 назви.

UDC 004.56:004.353.2

Studies on changes in the signal waveform in the channel of the monitor side electromagnetic radiation / *V.I. Zabolotny, E.V. Gerasimenko, V.I. Perepadya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 116 – 121.

The change of the response form of the induced EMF values in the reconnaissance device antenna in the SEMR far zone channel was demonstrated on the analysis of solutions of the Maxwell equations . It was established that the form of the EMF for the electric antenna corresponded to the second derivative of the original signal, and for the magnetic one it corresponded to the third derivative**.** Certain spectral functions of the signals studied using the properties of Fourier transforms**.** The possibility to determine the values of the initial signals parameters by the measured values of "zeros" of the SEMR spectrumwas shown**.**

Fig. 4. Ref.: 4 names.

УДК 681.323

Системы обнаружения и предотвращения вторжения / *А.А. Замула, В.Л. Морозов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 122 – 126.

Приведен анализ особенностей построения и применения систем обнаружения вторжений. Отмечаются сильные и слабые стороны таких систем, а также представлены факторы, которые необходимо учитывать при размещении и внедрении компонентов системы в сеть организации.

Ил. 1. Библиогр.: 3 назв.

УДК 681.323

Системи виявлення й запобігання вторгнення / *О.А. Замула, В.Л. Морозов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 122 – 126.

Наведено аналіз особливостей побудови та застосування систем виявлення вторгнень. Відзначаються сильні і слабкі сторони таких систем, а також представлені фактори, які необхідно враховувати при розміщенні та впровадженні компонентів системи в мережу організації.

Іл. 1. Бібліогр.: 3 назви.

UDC 681.323

Intrusion detection and prevention systems / *A.A. Zamula, V.L. Morozov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 122 – 126.

The analysis of the features of development and application of intrusion detection and prevention systems was carried out. Advantages and disadvantages of such systems were marked as well as the factors that should be considered during implementation and placement of the system components in an organization's network.

1 fig. Ref.: 3 items.

УДК 001.6+004

Влияние качества интернет-услуг на риски собственника компьютерной сети / *И.А. Громыко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 127 – 130.

Показан результат зависимости финансовых рисков владельца компьютерной сети от качества ее работы. Расчеты показывают, что ожидаемые потери финансов по причине ухудшения качества работы линии могут оказаться в два раза выше, чем считалось ранее. Этот факт является экономическим стимулом повышения качества компьютерной сети (лини связи).

Библиогр.: 6 назв.

УДК 001.6+004

Вплив якості інтернет-послуг на ризики власника комп'ютерної мережі / *І.А. Громико* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 127 – 130.

Показано результат залежності фінансових ризиків власника комп'ютерної мережі від якості її роботи. Розрахунки показують, що очікувані втрати фінансів з причини погіршення якості роботи лінії можуть виявитися в два рази вище, ніж вважалося раніше. Цей факт є економічним стимулом підвищення якості комп'ютерної мережі (лини зв'язку).

Бібліогр.: 6 назв.

UDC 001.6+004

Influence of internet service quality on risks of a computer network owner / *I.A. Gromyko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 127 – 130.

The influence of internet-service quality on risks of owner computer network is shown. Calculations show that the loss of finance, because of the quality deterioration can be twice as much. This fact is an economic incentive to improve the quality of computer network.

Ref.: 6 items.

СОВЕРШЕНСТВОВАНИЕ И РАЗВИТИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ
IMPROVEMENT AND DEVELOPMENT OF INFORMATION-TELECOMMUNICATION SYSTEM

УДК 004.75

Анализ формальной модели безопасности облака NIST / *И.Ф. Аулов, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 131 – 137.

Статья посвящена вопросам построения формальных моделей облака, моделей безопасности и их анализа. Рассматривается формальная модель облака, предложенная NIST, рассматриваются выделенные в облаке роли и их связи между собой, приводится описание основных функциональных компонентов облака и их функций. На основе данной модели проводится анализ модели безопасности облака, ее компонентов и функций безопасности которые должны быть реализованы в облаке. Анализируются связи между ролями, компонентами безопасности и сервисами облака. На основе проведеного анализа формальной модели облака и формальной модели безопасности облака NIST, сформулированы и предложены рекомендации по их усовершенствованию.

Ил. 2. Библиогр.: 5 назв.

УДК 004.75

Аналіз формальної моделі безпеки хмари NIST / *І.Ф. Аулов, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 131 – 137.

Стаття присвячена питанням побудови формальних моделей хмари, моделей безпеки і їх аналізу. Розглядається формальна модель хмари, запропонована NIST, розглядаються виділені в хмарі ролі та їх зв'язок між собою, наводиться опис основних функціональних компонентів хмари і їх функцій. На основі даної моделі проводиться аналіз моделі безпеки хмари, її компонентів і функцій безпеки які повинні бути реалізовані в хмарі. Аналізуються зв'язки між ролями, компонентами безпеки і сервісами хмари. На основі проведеного аналізу формальної моделі хмари і формальної моделі безпеки хмари NIST, сформульовано та запропоновано рекомендації з їх удосконалення.

Іл. 2. Бібліогр.: 5 назв.

UDC 004.75

Analysis of NIST formal cloud security model / *I.F. Aulov, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 131 – 137.

The questions of creation of cloud formal models, models of safety and their analysis are considered. A cloud formal model offered by NIST, the advanced roles in the cloud and their communication among themselvesare are presented, the main functional components of the clouds and their functions are given. Based on this model the analysis of cloud safety model, its components and safety functions which must be realized in thecloud is carried out. Communications between roles, components of safety and cloud services are analyzed. Based on the analysis of NIST cloud formal model and NIST cloud security modal, recommendations are formulated and suggestions concerning improvement of this models are put forward.

2 fig. Ref.: 5 items.

УДК 004.9

Электронная идентификация: понятие, определение, требования / *Ю.И.Горбенко, Ю.В.Гончарова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 138 – 144.

Рассматривается проблема определения электронной идентификации и пути ее решения. Приводится классификация существующих методов идентификации и аутентификации субъектов, общие требования к реализации внедрения электронной идентификации в Украине, как элемент разработки механизма электронных доверительных услуг.

Табл.3. Ил.2. Библиогр.: 6 назв.

УДК 004.9

Електронна ідентифікація: поняття, визначення, вимоги / *Ю.І. Горбенко, Ю.В. Гончарова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 138 – 144.

Розглядається проблема визначення електронної ідентифікації та шляхи її вирішення. Наводиться класифікація існуючих методів ідентифікації та автентифікації суб'єктів, загальні вимоги до реалізації впровадження електронної ідентифікації в Україні як елемент розробки механізму електронних довірчих послуг.

Табл.3. Іл.2. Бібліогр.: 6 назв.

UDC 004.9

Electronic identification: concept, definition, requirements / *Yu.I.Gorbenko, Yu.V.Goncharova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 138 – 144.

The problem of electronic identification definition and and the ways of its solution are considered. Classification of the available methods for identification and authentication of subjects, general requirements of electronic identification implementation in Ukraine, as as a part of development of electronic trust services mechanism are given.

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

УДК 681.3. 06 (07)

Сущность и необходимость выполнения дополнительных требований в отношении предоставления доверительных услуг в ЕС и Украине в период 2015 – 2030 рр. / *Ю.И. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 145 – 152.

Приводятся результаты анализа сущности, особенностей требований и механизмов реализации положений Регламента ЕС [3], изложенные в приложениях к нему, а также определение задач по их учету или виполнению при проектировании перспективных систем предоставления безопасных электронных услуг по электронной подписи, электронной печати, электронных документов , услуг электронной доставки и проверки подлинности веб - сайта.

Библиогр.: 7 назв.

УДК 681.3. 06 (07)

Сутність та необхідність виконання додаткових вимог відносно надання довірчих послуг в ЄС та Україні в період 2015 – 2030 рр. / *Ю.І. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 145 – 152.

Наведено результати аналізу сутності, особливостей вимог та механізмів реалізації положень Регламенту ЄС [3], що викладені в додатках до нього, а також визначення задач щодо їх врахування чи виконання при проектуванні перспективних систем надання безпечних електронних послуг щодо електронного підпису, електронної печатки, електронних документів, послуг електронної доставки та перевірки справжності веб – сайту.

Бібліогр.: 7 назв.

UDC 681.3. 06 (07)

The essence and the need to fulfill additional requirements for the provision of trustee services in the EU and Ukraine in the period of 2015 - 2030 / *Yu. I. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 145 – 152.

The results of analysis of the essence, requirements especially and mechanisms for implementation of the EC Regulation provisions, as set out in the annexes, as well as definition of the tasks on their account and implementation in the design of advanced systems to provide secure electronic services for electronic signature, electronic stamp, electronic documents, services of electronic delivery and authentication of the website are presented.

Ref.:7 items

УДК 004.75:004.05

Создание и анализ модели угроз в облачных вычислениях // *И.Д.Горбенко, М.И.Харламб* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 153 – 158.

Рассматривается строение системы облачных вычислений, состояние применения технологии, ее преимущества и недостатки. Определяется модель угроз в облачных вычислениях. Предлагается использование криптографической защиты информации при обмене данными через облако.

Табл.1. Ил.4. Библиогр.: 6 назв.

УДК 004.75:004.05

Створення та аналіз моделі загроз при обчисленнях в хмарі / *І.Д.Горбенко, М.І.Харламб* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 153 – 158.

Розглядається побудова системи хмарних обчислень, сучасний стан застосування технології, її переваги та недоліки. Визначається модель загроз в хмарних обчисленнях. Пропонується застосовування криптографічного захисту інформації при обміні даними через хмару.

Табл.1. Іл.4. Бібліогр.: 6 назв.

UDC 004.75:004.05

Creation and analysis of the threats model in cloud computing / *I.D. Gorbenko, M.I.Kharlamb* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 153 – 158.

The structure of the system of cloud computing, the usage of the technology, its advantages and disadvantages are considered. The threat model of cloud computing is defined. It is Pproposed to use the cryptographic information security in cloud computing.

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

УДК 621.391.7

Специализированные процессоры реализации цифрового подписания на основе рекуррентных последовательностей / *Ю.Е. Яремчук* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 159 – 163.

Представлены принципы построения специализированных процессоров реализации цифрового подписания на основе рекуррентных V_k-последовательностей. По сравнению с известными аналогами разработанные процессоры хоть и являются менее быстрыми, но обеспечивают больший уровень криптографической стойкости во время цифрового подписания, а также имеют большие возможности их применения в системах, использующих математический аппарат рекуррентных последовательностей.

Ил. 2. Библиогр.: 6 назв.

УДК 621.391.7

Спеціалізовані процесори реалізації цифрового підписування на основі рекурентних послідовностей / *Ю.Є. Яремчук* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 159 – 163.

Представлено принципи побудови спеціалізованих процесорів реалізації цифрового підписування на основі рекурентних V_k-послідовностей. У порівнянні з відомими аналогами розроблені процесори хоч і є менш швидкими, але забезпечують більший рівень криптографічної стійкості підчас цифрового підписування, а також надають більші можливості їх застосування у системах, що використовує математичний апарат рекурентних послідовностей.

Іл. 2. Бібліогр.: 6 назв.

UDC 621.391.7

Specialized processors realization of digital signature based on recurrent sequences / *Iu. Iaremchuk* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 159 – 163.

The principles of specialized processors realization of digital signature based on the V_k recurrent sequences are presented. As compared with the known analoguesthe developed processors although less speed, but provide a higher level of cryptographic reliability during digital signature, and also have larger possibilities of their application to the systems using mathematical apparatus recurrent sequences.

2 fig. Ref.: 6 items.

УДК 621.39, 004.7

Оценка влияния злонамеренного трафика на функционирование вычислительных решеток / *Д.А. Зайцев, Т.Р. Шмелева, В. Ретчитзеггер, Б. Пролл* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 164 – 171.

Построена модель прямоугольной коммуникационной решетки в форме раскрашенной сети Петри как композиция подмоделей терминальных устройств, производящих и потребляющих пакеты, и коммуникационных устройств, коммутирующих пакеты между терминальными устройствами. Модель дополнена пушками трафика, моделирующими злонамеренный трафик. Посредством имитационного моделирования в CPN Tools показано, что дуэль трафика пары пушек с нагрузкой менее пяти процентов от пиковой приводит решетку к полному тупику. Таким образом, показана уязвимость решеток к атакам трафиком. Направлением перспективных работ является противодействие атакам.

Табл. 3. Ил. 2. Библиогр.: 8 назв.

УДК 621.39, 004.7

Оцінка впливу зловмисного трафіку на функціонування обчислювальних ґраток / *Д.А. Зайцев, Т.Р. Шмельова, В. Ретчитзеггер, Б. Пролл* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 164 – 171.

Побудовано модель прямокутної комунікаційної гратки у вигляді розфарбованої сіті Петрі як композиція підмоделей термінальних пристроїв, що виробляють та споживають пакети, і комунікаційних пристроїв, що комутують пакети між термінальними пристроями. Модель доповнено гарматами трафіку, що моделюють зловмисний трафік. Через імітаційне моделювання в CPN Tools показано, що дуель трафіку пари гармат із навантаженням менш п’яти відсотків від пікового приводить гратку до повного тупику. Отже, показано уразливість граток до атак через трафік. Напрямком перспективних робіт є протидія атакам.

Табл. 3. Іл. 2. Бібліогр.: 8 назви.

UDC 621.39, 004.7

Evaluation of ill-intended traffic influence on computing grids functioning / *D.A. Zaitsev, T.R. Shmeleva, W. Retschitzegger, B. Proll* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – №176. – P. 164 – 171.

A rectangular communication grid model was constructed in the form of a colored Petri net as a composition of submodes of terminal devices producing and consuming packets and communication devices switching packets for their delivery among terminal devices. The model was supplied with traffic guns simulating ill-intended traffic. Via simulation in CPN Tools it was shown that a traffic duel of a pair of guns brings the grid to a full deadlock with less than five percent of the peak load. Thus, the vulnerability of grids to traffic attacks was revealed. The future work is aimed to resist the attacks.

3 tab. 2 fig. Ref.: 8 items.

ФИЗИКА ПРИБОРОВ И СИСТЕМ
PHYSICS OF DEVICES AND SYSTEMS№

УДК 681.7.069

Влияние поляризации оптического излучения на фототок различных моделей трап-детекторов / *Д.Н. Татьянко, Ю.П. Мачехин, К.А. Лукин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 172 – 180.

Поляризационная зависимость оптических трап-детекторв является одним из определяющих факторов, влияющих на точность измерений данным видом детекторов. В работе описывается модель поляризационной зависимости трап-детекторов. Найдена поляризационная зависимость и квантовая

эффективность различных конструкций трап-детекторов и проведен их сравнительный анализ. Предложена новая конструкция трап-детектора и показаны ее преимущества.

Табл. 7. Ил. 7. Библиогр.: 9 назв.

УДК 681.7.069

Вплив поляризації оптичного випромінювання на фотострум різних моделей трап-детекторів / *Д.М. Татьянко, Ю.П. Мачехин, К.О. Лукін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 172 – 180.

Поляризаційна залежність оптичних трап-детекторів є одним з визначальних факторів, що впливають на точність вимірювань даним видом детекторів. В роботі описується модель поляризаційної залежності трап-детекторів. Знайдена поляризаційна залежність і квантова ефективність різних конструкцій трап-детекторів і проведено їх порівняльний аналіз. Запропоновано нову конструкцію трап-детектора і показані її переваги.

Табл. 7. Іл. 7. Бібліогр.: 9 найм.

UDC 681.7.069

Influence of optical radiation polarization on photocurrent of different trap detectors models / *D. N. Tatyanko, Y. P. Machekhin, K. A. Lukin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – №176. – P. 172 – 180.

The polarization dependence of the optical trap detectors is one of the key factors affecting the accuracy of this type of detectors. The polarization dependence model of a trap detector is presented. Polarization dependences and quantum efficiencies of various trap detectors designs were simulated and comparated. The new trap detector design was presented and its advantage was shown.

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

УДК 535.2

Формирование оптических частотных реперов на основе фотонных кристаллов с дефектами и захваченных холодных атомов / *Ю. П. Мачехин, Е. Г. Меркулов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 181 – 186.

В настоящее время развитие оптических стандартов частоты ограничено только технической возможностью реализации частотных реперов. Одной из самых перспективных технологий формирования частотного репера является лазерное охлаждение атомов и ионов. В работе описывается возможность создания оптического репера на основе холодных атомов, захваченных в дефекты фотонных кристаллов. Рассматриваются особенность формирования поля в дефекте фотонного кристалла, условия загрузки атома в дефект фотонного кристалла оптическим пинцетом. Предложена новая конструкция реализации оптического репера на основе холодных атомов с использованием двух полей.

Ил. 2. Библиогр.: 12 назв.

УДК 535.2

Формування оптичних частотних реперів на основі фотонних кристалів з дефектами і захоплених холодних атомів / *Ю. П. Мачехін, Є. Г. Меркулов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 181 – 186.

В даний час розвиток оптичних стандартів частоти обмежено тільки технічною можливістю реалізації частотних реперів. Однією з найперспективніших технологій формування частотного репера є лазерне охолодження атомів і іонів. В роботі описується можливість створення оптичного репера на основі холодних атомів, захоплених в дефекти фотонних кристалів. Розглядаються особливість формування поля в дефекті фотонного кристала, умови завантаження атома в дефект фотонного кристала оптичним пінцетом. Запропоновано нову конструкцію реалізації оптичного репера на основі холодних атомів з використанням двох полів.

Іл. 2. Бібліогр.:12 назв.

UDC 535.2

Generation of optical frequency bench mark based on photonic crystals with defects and trapped cold atoms / *Y. P. Machekhin, E. G. Merkulov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 181 – 186.

At present, the development of optical frequency standards is limited only by the technical ability of the frequency bench marks. One of the most promising technologies is the formation of frequency bench marks with laser cooling of atoms and ions. This paper describes the ability of an optical bench mark based on cold atoms trapped in defects in photonic crystals. We consider the feature of formation the field in defect

of the photonic crystal, the conditions of loading of an atom in a defect photonic crystal by optical tweezers. New construction of realization of optical bench mark based on cold atoms using two fields is suggested.

Fig. 2. Ref.: 12 items.

УДК 537.635

Комплекс для исследования наноразмерных магнетиков методом сверхвысокочастотного электронного парамагнитного резонанса / *А. С. Вакула, С. В. Недух, С. И. Тарапов, С. Ю. Полевой* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 187 – 190.

Представлены особенности конструкции ЭПР спектрометра «КВАРК», в котором с целью повышения чувствительности и информативности эксперимента разработана схема программного управления, а также регистрации данных с помощью звуковой карты ПК с пакетом специально разработанных авторских программ (система «Sonic»), работающей как синхродетектор. Также в статье представлены результаты работы системы Sonic в сравнении с результатами работы магнитного спектрометра, в котором функцию СВЧ генератора и регистрирующего устройства выполняет прецизионный серийно выпускаемый векторный анализатор цепей Agilent NA5230A, имеющий автоматическую перестройку частоты.

УДК 537.635

Комплекс для дослідження нанорозмірних магнетиків методом надвисокочастотного електронного парамагнітного резонансу / *А. С. Вакула, С. В. Недух, С. І. Тарапов, С. Ю. Полевой* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 187 – 190.

Представлено особливості конструкції ЕПР спектрометра «КВАРК», в якому з метою підвищення чутливості й інформативності експерименту розроблена схема програмного керування, а також реєстрації даних за допомогою аудіокарти ПК з пакетом спеціально розроблених авторських програм (система «Sonic»), ярий працює як сінхродетектор. Також у статті представлені результати роботи системи Sonic в прівнянні з результатами роботи магнітного спектрометра, в якому функцію НВЧ генератора і пристрою який реєструє виконує прецизійний серійно випускаємий векторний аналізатор кіл Agilent NA5230A, який має автоматичну перестройку частоти.

UDC 537.635

Complex of nanoscale magnetic materials study by microwave electron spin resonance method / *A. S. Vakula, S. V. Nedukh, S. I. Tarapov, S. Yu. Polevoy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 187 – 190.

The designed features of the ESR spectrometer "Quark" are present. The scheme, software management and data registration via the PC sound card with a package of specially authoring software (system «Sonic») as sync detector operating are developed to improve the sensitivity of the information content of the experiment. Also the results of the work of Sonic in comparison with the results of the magnetic spectrometer, in which the function of the microwave generator and the recording device performs precision commercially available vector network analyzer Agilent NA5230A, having automatic frequency tuning is presented.

УДК 628-1/-9

Квантово-механический подход к определению параметров нанофотонного сенсора при детектировании 3,4-бензпирена / *О.А. Сушко, И.В. Мукановская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 191 – 199.

Представлена физическая модель процессов, протекающих в нанофотонном сенсоре на основе сферических полупроводниковых квантовых точек при определении 3,4-бензпирена в водных объектах окружающей среды. На основе данной модели проведены квантово-химические расчеты электронной структуры 3,4-бензпирена и расчет зависимости ширины запрещенной зоны сферической полупроводниковой квантовой точки от ее радиуса. На основе проведенных расчетов был осуществлен выбор оптимального материала и диаметра сферических полупроводниковых квантовых точек при использовании их как детекторных элементов нанофотонного сенсорного устройства для определения 3,4-бензпирена в водных объектах окружающей среды.

Ил. 4. Библиогр.: 12 назв.

УДК 628-1/-9

Квантово-хімічний підхід до визначення параметрів нанофотонного сенсора при детектуванні 3,4-бензпірену / *О.А. Сушко, І.В. Мукановська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 191 – 199.

Представлено фізичну модель процесів, що протікають у нанофотонному сенсорі на основі сферичних напівпровідникових квантових точок при визначенні 3,4-бензпірена у водних об'єктах довкілля. На основі даної моделі проведені квантово-хімічні розрахунки електронної структури 3,4-бензпірена та розрахунок залежності ширини забороненої зони сферичної напівпровідникової квантової точки від її радіуса. На основі проведених розрахунків здійснений вибір оптимального діаметру та матеріалу сферичних напівпровідникових квантових точок при використанні їх як детекторних елементів нанофотонного сенсорного пристрою для визначення 3,4-бензпірена у водних об'єктах довкілля

Іл. 4. Бібліогр.: 12 назв

UDC 628-1/-9

Quantum-mechanical approach to determination of nanophotonic sensor parameters during 3,4-benzpyrene detection / *O.A. Sushko, I.V. Mukanovska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 191 – 199.

The physical model of the processes occurring in nanophotonic sensor based on spherical semiconductor quantum dots in 3,4-benzpyrene detection in environmental water objects is presented. Quantum chemical calculations of the 3,4-benzpyrene electronic structure and semiconductor spherical quantum dot band gap dependence computer simulation on its radius are conducted on the basis of the presented model. Selection of the optimal material and diameter spherical semiconductor quantum dots for use as detector elements of nanophotonic sensor device for 3,4-benzpyrene detection in water objects of environmental has been carried out on the basis of the calculations.

4 fig. Ref.: 12 items.

ЭЛЕКТРОДИНАМИКА
ELECTRODYNAMICS

УДК 539.27

Дифракция электронов при наклонном падении на решетку бесконечно тонких металлических лент / *А.В.Безуглый, А.М.Петченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 200 – 204.

Предлагается квантовомеханическая модель явления дифракции электронов на решетке из бесконечно тонких металлических лент. Исходя из предположения о том,что электроны, проходя через щели, взаимодействуют с электронами вещества, показано, что вид дифракционной картины, наблюдаемой на экране, определяется спектром импульсов электронов вещества из которого изготовлені ленты. Получено соотношение, определяющее дифракционные углы, под которыми наблюдаются максимумы освещенности, совпадающее в случае малых углов дифракции и больших углов скольжения с известным уравнением дифракционной решетки.

Ил.3. Библиогр.:4 назв.

УДК 539.27

Дифракція електронів при похилому падінні на гратку нескінченно тонких металевих стрічок / *А.В. Безуглий*, *О.М. Петченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 200 – 204.

Пропонується квантовомеханічна модель явища дифракції на одновимірній гратці із нескінченно тонких металевих стрічок. Виходячи з припущення, що електрони, які проходять через щілини, взаємодіють з електронами речовини, показано, що вид дифракційної картини, яка спостерігається на екрані, визначається врешті решт спектром импульсів електронів речовини з якої виготовлені пластини. Отримано співвідношення, що визначає дифракційні кути, під якими спостерігаються максимуми освітленості, яке у випадку малих кутів дифракції та великих кутів ковзання збігається з відомим рівнянням дифракційної гратки.

Іл.3.Бібліогр.4 назв.

UDC 539.27

Diffraction of electrons on the grating of infinitely thin metallic strips at the inclined incidence / *A.V. Besougly, A.M.Petchenco* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 200 – 204.

The quantum mechanics model of the electrons diffraction on the one-dimensional grating of the infinitely thin strips is proposed. Supposing that photons flighting through the slits interect with electrons of a solid, it is demonstrated that the diffraction pattern is determinated by the spectrum of momentums of electrons. The expression determining diffraction angles of scattered electrons coinsiding in the case of small diffraction angles and grate of slip angles with known equation of diffraction grating is obtaind.

3fig.Ref.:4 items.

УДК 537.87

Передача субволнового изображения проволочной линзой с фазовой компенсацией в миллиметровом диапазоне длин волн / *Л.И. Кожара, С.Ю.Полевой, Д.С.Филонов, С.И. Тарапов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 205 – 209.

Статья посвящена экспериментальному исследованию процессов передачи распределения электромагнитного поля от двух рядом расположенных точечных источников в проволочной линзе, снабженной диэлектрическим фазовым компенсатором. Измерены спектральные характеристики проволочной линзы в частотном диапазоне 2-24 *ГГц*. Экспериментально продемонстрировано явление концентрации электромагнитной энергии проволочной линзой и проанализированы ее фокусирующие свойства. Также экспериментально продемонстрирована возможность передачи субволнового изображения проволочной линзой со встроенным фазовым компенсатором с разрешающей способностью около λ/15.

УДК 537.87

Передача субхвильового зображення дротяною лінзою з фазовою компенсацією у міліметровому діапазоні довжин хвиль / *Л.І. Кожара, С.Ю. Полевой, Д.С. Філонов, С.І. Тарапов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 205 – 209.

Стаття присвячена експериментальному дослідженню процесів передачі розподілу електромагнітного поля від двох розташованих поруч точкових джерел у дротяній лінзі з вбудованим діелектричним фазовим компенсатором. Виміряно спектральні характеристики дротяної лінзи в частотному діапазоні 2-24 *ГГц*. Експериментально продемонстровано явище концентрації електромагнітної енергії дротяною лінзою та проаналізовані її фокусуючі властивості. Також експериментально продемонстрована продемонстрована можливість передачі субхвильового зображення дротяної лінзою із вбудованим фазовим компенсатором з роздільною здатністю близько λ/15.

UDC 537.87

Transmission of subwavelength image by wire lens with phase compensation in the millimeter wavelength range / *L. Kozhara, S. Polevoy, D. Filonov, S. Tarapov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 205 – 209.

The paper is devoted to the experimental investigation of the transmission processes of electromagnetic field distribution from two near located point sources in the wire lens with the embedded dielectric phase compensator. The spectral characteristics of wire lens in the frequency range 2-24 GHz are measured. The experimental technique of measuring the characteristics is realized. The ability to transfer subwavelength images by wire lens with embedded phase compensator with a resolution λ/15 is demonstrated experimentally.

УДК 537.622.4

Поверхностные электромагнитные состояния и левосторонние свойства в структуре фотонный кристалл – феррит – плазмоподобная среда / *А. А. Харченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 210 – 213.

Ввиду возможности применения поверхностных электромагнитных состояний (ПЭМС), так называемых таммовских состояний (ТС), в современных электронно-управляемых СВЧ устройствах актуальной остается задача об управлении характеристиками этих устройств с помощью внешних параметров. Поэтому, в настоящей работе экспериментально изучена зависимость спектра пропускания структуры фотонный кристалл/феррит/плазмоподобная среда от внешнего постоянного магнитного поля и температуры. Интересным является тот факт, что для исследуемой структуры в некоторых облас-

тях частот (где оба материальных параметра будут принимать отрицательные значения) наблюдается переход отТСк «левостороннему» характеру спектра (ЛС-пику). Кроме того, на высоких полях мы наблюдаем возникновение обеих особенностей спектра, а именно, и ТС, и ЛС-пик. Именно исследованию этих особенностей и посвящена данная статья.

УДК 537.622.4

Поверхневі електромагнітні стани та лівосторонні властивості в структурі фотонний кристал – ферит – плазмоподібне середовище / *Г.О. Харченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 210 – 213.

Через можливість застосування поверхневих електромагнітних станів (ПЕМС), так званих таммівських станів (ТС), в сучасних електронно-керованих НВЧ пристроях актуальною залишається задача про керування характеристиками цих пристроїв за допомогою зовнішніх параметрів. Тому, в даній роботі експериментально досліджена залежність спектра пропускання структури фотонний кристал/ферит/плазмоподібне середовище від зовнішнього постійного магнітного поля і температури. Цікавим є той факт, що для досліджуваної структури в деяких областях частот (де обидва матеріальних параметра прийматимуть від'ємні значення) спостерігається перехід від ТС до «лівостороннього» характеру спектра (ЛС-піку). Крім того, на високих полях ми спостерігаємо виникнення обох особливостей спектра, а саме, і ТС, і ЛС-пік. Саме дослідженню цих особливостей і присвячена ця стаття.

UDC 537.622.4

Surface electromagnetic states and left-hand properties of the photonic crystal – ferrite – plasma-like media structure / *G.O.Kharchenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 210 – 213.

Using the surface electromagnetic states (SEMS) of the so called Tamm states (TS) in the modern electronically controlled microwave devices the task of control of these devices characteristics with external parameters. Therefore, we experimentally investigated the dependence of the transmission spectrum of the photonic crystal/ferrite/plasma-like media structure on the external magnetic field and temperature. It is interesting to know that the structure under study in some frequency range (where both material parameters will be negative) transition from TS to "left-hand" nature of the spectrum (LH-peak)is observed. In addition, at high fields, we observed the appearance of two features of the spectrum, namely, TS and LH-peak, simultaneously. This paper is devoted to investigations into these features.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ
TELECOMMUNICATIONS SYSTEMS AND NETWORKS

УДК 621.391

Модель маршрутизации и распределения канальных ресурсов WiMaxmesh-сети / *О.Ю. Евсеева, Э. М. Аль-Аззави* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 214 – 220.

Предложена математическая динамическая модель, описывающая беспроводную сеть стандарта 802.16 режима mesh в пространстве состояний. Модель нацелена на совместное решение задач маршрутизации и управления канальными ресурсами таких сетей путем оптимального распределения временных слотов канального уровня. Модель учитывает ограниченность канальных и буферных ресурсов, явление интерференции, возможность повторного использования слотов и обеспечивает трактовку рассматриваемых задач в рамках теории оптимального управления.

Ил. 3. Библиогр.: 13 назв.

УДК 621.391

Модель маршрутизаціїтарозподілу канальних ресурсів WiMaxmesh-мережі / *О.Ю.Євсєєва, Е. М. Аль-Аззаві* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 214 – 220.

Запропоновано математичну динамічну модель, що описує бездротову мережу стандарту 802.16 режиму mesh в просторі станів. Модель націлена на одночаснерозв'язання задач маршрутизації та управління канальними ресурсами таких мереж шляхом оптимального розподілу часових слотів канального рівня. Модель враховує обмеженість канальних і буферних ресурсів, явище інтерференції, можливість повторного використання слотів і забезпечує трактування розглянутих задач в рамках теорії оптимального управління.

Іл. 3. Бібліогр.: 13 назв.

UDC 621.391

Model of routing and scheduling in WiMaxmesh-network / *O.Yu. Yevsyeyeva, E.M. Al-Azzawi* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 214 – 220.

A mathematical dynamic model on wireless 802.16 mesh network in the state space is offered. The model is aimed at joint solution of the tasks of channel resources routing and control in such networks through optimal allocation of time slots on the link layer. The model takes into account the limited channel and buffer resources, the interference between stations, makes it possible to reuse slot reuse and provides interpretation of the problems in the framework of the optimal control theory.

3 fig. Ref.: 13items.

УДК 621.391

Модель выделения требуемой скорости передачи в нисходящем канале связи технологии LTE / С.*В. Гаркуша, Е.В. Гаркуша* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 221 – 228.

Приведены результаты разработки математической модели распределения подканалов нисходящего канала связи технологии LTE. Предложенная модель направлена на обеспечение гарантированного качества обслуживания пользователей беспроводной сети путем выделения пользовательской станции требуемой скорости передачи в нисходящем канале связи. Проведен сравнительный анализ предложенной модели с существующими методами распределения радиоресурса технологии LTE с точки зрения обеспечения общей производительности нисходящего канала связи, степени балансировки пропускной способности, а также вероятности выделения пользовательским станциям требуемой скорости передачи.

Табл. 1. Ил. 5. Библиогр.: 14 назв.

УДК 621.391

Модель виділення необхідної швидкості передачі в низхідному каналі зв'язку технології LTE / С.*В. Гаркуша, О.В Гаркуша* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 221 – 228.

Наведено результати розробки математичної моделі розподілу підканалів низхідного каналу зв’язку технології LTE. Запропонована модель спрямована на забезпечення гарантованої якості обслуговування користувачів безпроводової мережі шляхом виділення користувацькій станції необхідної швидкості передачі в низхідному каналі зв’язку. Проведено порівняльний аналіз запропонованої моделі з існуючими методами розподілу радыоресурсу технології LTE з точки зору забезпечення загальної продуктивності низхідного каналу зв’язку, ступеня балансування пропускної здатності, а також ймовірності виділення користувацьким станціям необхідної швидкості передачі.

Табл. 1. Іл. 5. Бібліогр.: 14 назв.

UDC 621.391

Model for the desired transmission rate selection in the downlink technology LTE / S.*V. Garkusha, O.V. Garkusha* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 221 – 228.

The results of development of the mathematical model subchannel allocation downlink technology LTE are given. The proposed model is aimed at providing the guaranteed quality of service to wireless users by allocating the user station required transmission rate in the downlink. A comparative analysis is carried out of the proposed model with existing methods of radio resource distribution LTE technology in terms of the overall performance of downlink power balancing capacity, as well as the probability of selection subscrieber stations required transmission rate.

1 tab. 5 fig. Ref.: 14 items.

УДК 621.391.31

Исследование влияния самоподобного трафика на показатели качества передачи речи в информационно-телекоммуникационных системах / *Фуад Вехбе, С.А.Заводов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 229 – 234.

Современные телекоммуникационные сети развиваются в направлении перехода к мультисервисным сетям обеспечивающих передачу больших разновидностей потоков. При этом используемые классические модели потоков, основанные на пуассоновских процессах потеряли свою адекватность в условиях возросшей сложности функционирования современных сетей. Как показали исследования более точно эти процессы могут быть описаны моделями самоподобных процессов. Это требует проведения дополнительных исследований на правленых на изучения функционирования мультисервис-

ных сетей в условиях самоподобного трафика. Одним из видов трафика, к которому проявляется наибольший интерес, является передача потоков реального времени к которым относится трафик телефонии.

Проведено исследование влияния самоподобия трафика телефонии (передача речи) на параметры качества обслуживания (задержка и вероятность потерь) и на параметры субъективного восприятия.

Ил.4. Библиогр.: 10 назв.

УДК 621.391.31

Дослідження впливу самоподібного трафіку на показники якості передачі мови в інформаційно-телекомунікаційних системах / *Фуад Вехбе, С.О.Заводов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 229 – 234.

Сучасні телекомунікаційні мережі розвиваються в напрямку переходу до мультисервісних мереж, що забезпечують передачу великого різновиду потоків. При цьому класичні моделі потоків, що використовуються зараз та які засновані на пуассонівських процесах втратили свою адекватність в умовах великої складності функціонування сучасних мереж. Як показали дослідження трафіку більш точно ці процеси можуть бути описані моделями самоподібних процесів. Це вимагає проведення додаткових досліджень, що направлені на вивчення функціонування мультисервісних мереж в умовах самоподібного трафіку. Одним з видів трафіку, до якого проявляється найбільший інтерес є передача потоків реального часу до яких відноситься трафік телефонії.

Проведено дослідження впливу самоподібності трафіку телефонії (передача мови) на параметри якості обслуговування затримка і ймовірність втрат)та на параметри суб'єктивного сприйняття.

Іл. 4. Бібліогр.: 10 назв.

UDC 621.391.31

Investigation of self-similar traffic influence on the voice transmission quality in information and telecommunication systems / *Fouad Wehbe, S.A.Zavodov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – №176. – P. 229 – 234.

Modern telecommunication networks evolve toward transition to multi-service networks capable of delivering a high variety of flows. In this case the classic flows' models based on Poisson process lost their adequacy in terms of a great difficulty of modern networks functioning. As the investigations have shown these processes can be described more accurately by the model of self-similar processes. This requires additional research aimed at studying the functioning of multi-service networks under conditions of self-similar traffic. One of the types of traffic, which reveals itself the most interesting, is the transmission of real-time flows which include the telephony traffic.

The influence of self-similarity of traffic telephony (voice) on the parameters of quality of service delay and loss probability) and the parameters of subjective perception is studied.

4 fig. Ref.: 10 items.

ОБРАБОТКА СИГНАЛОВ
SIGNAL PROCESSING

УДК 658.513.012.12

Задача построения адекватного математического описания процесса преобразования сигнала в электронно-измерительной системе / *С.К. Мещанинов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 235 – 241.

Представлено рішення задачі адекватного математичного опису процесу перетворення сигналу в електронно-вимірювальній системі з метою забезпечення його максимальної надійності і достовірності. Розглянути особливості поставленого завдання і запропонований метод знаходження стійкого рішення. Для досягнення поставленої мети побудована модель зовнішньої дії на електронно-вимірювальну систему.

Библиогр.: 8 назв.

УДК 658.513.012.12

Завдання побудови адекватного математичного опису процесу перетворення сигналу в електронно-вимірювальній системі / *С.К. Мещанінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 235 – 241.

Представлено рішення задачі адекватного математичного опису процесу перетворення сигналу в електронно-вимірювальній системі з метою забезпечення його максимальної надійності і достовірності. Розглянуті особливості поставленого завдання і запропонований метод знаходження стійкого рішення. Для досягнення поставленої мети побудована модель зовнішньої дії на електронно-вимірювальну систему.

Бібліогр. 8 назв.

UDC 658.513.012.12

Problem of constructing an adequate mathematical description of the signal shaping process in the electronic-measuring system / *S.K.Meshaninov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 235 – 241.

Solution of the problem of an adequate mathematical description process of the signal shaping is presented in the electronic - measuring system to provide themaximal reliability and authenticity. The feature of the specified problem and the method being steady offered the decision of the problem. To achieve the set purpose the model of the external action on the electronic measuring system is built.

Ref 8 items

УДК 621.396.96: 551.508.855: 519.254

Системы обработки сигналов в режиме реального времени / *А.И.Литвин-Попович* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 242 – 246.

Рассмотрены вопросы реализации обработки сигналов в режиме реального времени на основе вычислительных систем общего назначения. Показана возможность реализации систем обработки с заданными вероятностными показателями времени обработки. При этом в качестве вычислительных устройств рассматриваются универсальные и графические процессоры современных персональных компьютеров. Результаты проиллюстрированы натурными экспериментами.

Ил. 5. Библиогр.: 6 назв.

УДК 621.396.96: 551.508.855: 519.254

Системи обробки сигналів в режимі реального часу / *А.І.Литвин-Попович* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 242 – 246.

Розглянуто питання реалізації обробки сигналів в режимі реального часу на основі обчислювальних систем загального призначення. Показано можливість реалізації систем обробки з завданими імовірнісними покажчиками часу обробки. При цьому в якості обчислювальних пристроїв розглядаються універсальні та графічні процесори сучасних персональних комп'ютерів. Результати проілюстровано натурними експериментами.

Іл. 5. Бібліогр.: 6 назв.

UDC 621.396.96: 551.508.855: 519.254

Signal processing systems in real-time mode / *A.I.Lytvyn-Popovych* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 242 – 246.

Building of the real-time signal processing systems on a basis of general-purpose hardware and software has been discussed. Realization of a signal processing system with given probabilistic characteristics has been illustrated. General-purpose and graphical processors of modern personal computers were used as computational devices. Results were illustrated by an experiment.

5 fig. Ref.: 6 items.

РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА И СРЕДСТВА ТЕЛЕКОММУНИКАЦИИ
RADIO ENGINEERING DEVICES AND TRLRCOMMUNICATIONS MEANS

УДК 621.317

Сравнительный анализ погрешности многозондовых микроволновых мультиметров с обработкой методами фильтра Калмана и наименьших квадратов, учитывающий переотражения зондов / *О.Б. Зайченко, И.И. Ключник, М.А. Мирошник, Р.И. Цехмистро* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 247 – 252.

Рассмотрена погрешность, вносимая переотражениями между датчиками в погрешность многозондового микроволнового мультиметра. Расстояние между датчиками соответствует $\lambda_в/8$ ($\lambda_в$ – длина волны в волноводе). Это значит, что соседние датчики влияют друг на друга. Рассмотрено одномер-

ное и двумерное размещение датчиков. Построена математическая модель с использованием направленных графов. Получена система линейных алгебраических урвнений, слагаемые которых учитывют переотражения между датчиками. При оценке погрешности мощности и других параметров, измеряемых многозондовым микроволновым мультиметром, применяется усреднение методом наименьших квадратов (МНК) и фильтр Калмана. Полученные результаты позволяют в дальнейшем быстро перейти к автоматизации процесса измерений.

УДК 621.317

Порівняльний аналіз похибки багатозондового мікрохвильових мультиметров з обробкою методами фільтра Калмана і найменших квадратів, що враховує переотраженія зондів / *О.Б. Зайченко, І.І. Ключник, М.А. Мірошник, Р.І. Цехмістро* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 247 – 252.

Розглянуто похибку, яка вноситься перевідбиттям між датчиками в похибку багатозондового мікрохвильового мультиметра . Відстань між датчиками відповідає λв / 8 (λв - довжина хвилі в хвилеводі). Це означає , що сусідні датчики впливають один на одного. Розглянуто одномірне і двовимірне розміщення датчиків. Побудовано математичну модель з використанням спрямованих графів. Отримано систему лінійних алгебраїчних урвненій, доданки яких враховують перевідбиття між датчиками. При оцінці похибки потужності та інших параметрів, вимірюваних багатозондового мікрохвильовим мультиметром, застосовується усереднення методом найменших квадратів (МНК) і фільтр Калмана. Отримані результати дозволяють надалі швидко перейти до автоматизації процесу вимірювань .

UDC 621.317

Comparative analysis of the multiprobe microwave multimeters errors with methods of Kalman filter and least squares proceesing, taking into account the multireflection of probes / *O.B. Zaychenko, I. I. Klyuchnyk, M.A. Miroshnik, R.I. Tsekhmistro* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 247 – 252.

This article describes the partial error introduced by reflections between the sensors in multiprobe microwave multimeter error. Distance between the sensors corresponds λw / 8 (λw - wavelength in the waveguide). This means that neighboring sensors influence each other. A one-dimensional and two-dimensional arrangement of sensors was considered. A mathematical model using directed graphs was worked out. A system of linear algebraic equation, terms which account on multireflection between sensors was built. There was used an averaging method of least squares (LS) and the Kalman filter in assessing the accuracy of power and other parameters measured by multiprobe microwave multimeter. The obtained results allow us to move quickly to further automation of the measurement process.

УДК 621.391

Анализ энергопотребления модулей для беспроводных сенсорных сетей стандарта IEEE 802.15.4 / *И.С. Шостко, Ю.Э. Соседка* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 253 – 257.

Рассматриваются распределенные самоорганизующиеся многоячеистые сети, базирующиеся на стандарте IEEE 802.15.4 с низкой скоростью передачи данных и сверхнизким энергопотреблением узлов. Основной сферой применения беспроводных сенсорных сетей (БСС) является сбор по беспроводному каналу связи показаний от множества датчиков, распределенных в пространстве. Приводятся примеры особенностей расчёта энергопотребления модулей БСС, пример математической модели энергопотребления БСС предназначенной для оценки средней мощности потребления узлов. Задача статьи показать, что разумный выбор элементной базы и ее правильная настройка поможет построить распределенную беспроводную сеть с долгим бесперебойным сроком службы.

Ил. 4. Библиогр.: 8 назв.

УДК 621.391

Аналіз енергоспоживання модулів для безпроводових сенсорних мереж стандарту IEEE 802.15.4 / *І.С. Шостко, Ю.Е. Сосєдка* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 253 – 257.

Розглядаються розподілені самоорганізуючі багатоячійкові мережі, що базуються на стандарті IEEE 802.15.4 з низькою швидкістю передачі даних і наднизьким енергоспоживанням вузлів. Основною сферою застосування безпроводових сенсорних мереж (БСС) є збір по безпроводовому каналу зв'язку свідчень від безлічі датчиків, розподілених в просторі. Наведено приклади особливостей розрахунку енергоспоживання модулів БСС, приклад математичної моделі енергоспоживання БСС призначеної для оцінки середньої потужності споживання вузлів. Завдання статті показати, що ро-

зумний вибір елементної бази та її правильне налаштування допоможе побудувати розподілену безпроводову мережу з довгим безперебійним терміном служби.

Іл.4. Бібліогр.: 8 назв.

UDC 621.391

Power analysis modules for wireless sensor networking standard / *I.S. Shostko, J.E. Sosedka* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 253 – 257.

The article deals with the distributed self-organizing multicellular networks based on the standard IEEE 802.15.4 low data rate and ultra low power consumption of nodes. The main scope of wireless sensor networks (WSN) is a collection of wirelessly readings from multiple sensors distributed in space. The article gives examples of features of WSN energy analysis modulesthere is an example of the mathematical model of energy WSN designed to estimate the average power consumption of nodes. The goal of this article is to show that a reasonable choice of the element base and its proper setting will help to build a distributed wireless network with a long trouble free service.

Il. 4. Ref.: 8 items.

УДК 621.3.072.6

Математическая модель быстродействующей самонастраиваемой нелинейной системы фазовой автоподстройки частоты / *С.А. Макаров, О.Н. Чекунова, С.А. Юхновский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2014. – Вып. 176. – С. 258 – 261.

На основе структурного и параметрического синтеза предложено математическую модель оптимальной по быстродействию самонастраиваемой системы ФАП, которая описывается нелинейным дифференциальным уравнением четвертого порядка. Повышение быстродействия данной модели достигается регулированием коэффициента усиления в цепи дополнительной обратной связи за законом вида $\sqrt[4]{x}$.

Табл. 1. Ил. 1. Библиогр.: 3 назв.

УДК 621.3.072.6

Математична модель швидкодіючої самонастроювальної нелінійної системи фазового автопідстроювання частоти / *С.А. Макаров, О.М. Чекунова, С.А. Юхновський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2014. – Вип. 176. – С. 258 – 261.

На основі структурного та параметричного синтезу запропоновано математичну модель оптимальної по швидкодії самонастроювальної системи ФАП, яка описується нелінійним диференційним рівнянням четвертого порядку. Підвищення швидкодії даної моделі досягається регулюванням коефіцієнта підсилення в колі додаткового зворотного зв’язку за законом виду $\sqrt[4]{x}$.

Табл. 1. Іл. 1. Бібліогр.: 3 назви.

UDC 621.3.072.6

Mathematical model of high-speed self-adaptive nonlinear system of phase lock / *S. A. Makarov, O.N. Chekunova, S.A. Yukhnovsky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2014. – № 176. – P. 258 – 261.

The mathematical model of optimal in the séance of speed of the self-adaptive phase lock which is described of nonlinear differential equation of fourth order is proposed based on the structural and parametric synthesis. Improving the performance of this model is achieved by control of gain in the chain of additional feedback by the law of $\sqrt[4]{x}$.

Tabl. 1. Il. 1. Ref.: 3 items.