МЕТОДИ ПЕРСПЕКТИВНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ
МЕТОДЫ ПЕРСПЕКТИВНИХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ
METHODS OF PROMISING CRYPTOGRAPHIC TRANSFORMATIONS

УДК 004.056.55

Обґрунтування та пропозиції щодо вибору, удосконалення та стандартизації механізму постквантового електронного підпису на національному та міжнародному рівнях / *І.Д. Горбенко, О.Г. Качко, О.В. Потій, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, І.В. Стельник, С.О. Кандій, К.О.Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 5 – 26.

Наразі та в перспективі для криптографічного захисту інформації застосовуються та будуть застосовуватись математичні методи, механізми та алгоритми стандартизованих асиметричних криптоперетворень типу електронний підпис (ЕП). Електронний підпис є основною та суттєвою складовою забезпечення кібербезпеки у сенсі якісного надання таких послуг з безпеки інформації як цілісність, неспростовність та автентичність інформації та даних, що обробляються. Але є реально обґрунтовані підозри, що у постквантовий період існуючі стандарти ЕП будуть зламуватись та компрометуватись з використанням класичних та квантових криптоаналітичних систем з відповідним математичним, програмним та апаратно-програмним забезпеченням. Проведено аналіз, що підтверджує, що уже практично розроблені, виготовлені та застосовуються квантові комп'ютери. При цьому вважається, що фактичний стан розроблення та застосування потужних квантових комп'ютерів та їх математичного і програмного забезпечення є, очевидно, строго конфіденційним та надійно захищається, а розголошуються тільки явно відомі дані про квантові комп'ютери та їх можливості застосування в криптології. Проведено попередній аналіз, який показує, що в Україні є розуміння існування загроз кібербезпеці та безпеці інформації у випадку застосування у перехідний та постквантовий періоди існуючих стандартизованих ЕП. Одним із основних проблемних питань щодо забезпечення необхідних рівнів безпеки в перехідний та постквантовий періоди є також розробка та прийняття постквантових стандартів ЕП. Метою статті є обґрунтування, порівняння альтернатив та розробка пропозицій щодо вибору та стандартизації постквантових стандартів ЕП на міжнародному та національному рівнях з урахування результатів 2-го та 3-го раундів конкурсу NIST США та національних досліджень.

Ключові слова: електронний підпис; криптографічний захист інформації; постквантовий період; «Сокіл»; Falcon; NIST PQC.

Табл. 4. Іл. 4. Бібліогр.: 35 назв.

УДК 004.056.55

Обоснование и предложения по выбору, усовершенствованию и стандартизации механизма постквантовой электронной подписи на национальном и международном уровнях / *И.Д. Горбенко, Е.Г. Качко, А.В. Потий, Ю.И. Горбенко, В.А. Пономарь, М.В. Есина, И.В. Стельник, С.О. Кандий, Е.А.Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 5 – 26.

В настоящее время и в перспективе для криптографической защиты информации применяются и будут применяться математические методы, механизмы и алгоритмы стандартизированных асимметричных криптопреобразований типа электронная подпись (ЭП). Электронная подпись является основной и существенной составляющей обеспечения кибербезопасности в смысле качественного предоставления таких услуг по безопасности информации как целостность, неопровержимость и подлинность информации и обрабатываемых данных. Но есть реально обоснованные подозрения, что в постквантовый период существующие стандарты ЭП будут взламываться и компрометироваться с использованием классических и квантовых криптоаналитических систем с соответствующим математическим, программным и аппаратно-программным обеспечением. Проведен анализ, подтверждающий, что практически разработаны, изготовлены и применяются квантовые компьютеры. При этом считается, что фактическое состояние разработки и применения мощных квантовых компьютеров и их математического и программного обеспечения, очевидно, строго конфиденциально и надежно защищается, а разглашаются только явно известные данные о квантовых компьютерах и их возможности применения в криптологии. Проведен предварительный анализ, показывающий, что в Украине есть понимание существования угроз кибербезопасности и безопасности информации в случае применения в переходной и постквантовый периоды существующих стандартизированных ЭП. Одним из основных проблемных вопросов обеспечения необходимых уровней безопасности в переходной и постквантовый периоды является также разработка и принятие постквантовых стандартов ЭП. Цель статьи – обоснование, сравнение альтернатив и разработка предложений по выбору и стандартизации постквантовых стандартов ЭП на международном и национальном уровнях с учетом результатов 2-го и 3-го раундов конкурса NIST США и национальных исследований.

Ключевые слова: электронная подпись; криптографическая защита информации; постквантовый период; «Сокіл»; Falcon; NIST PQC.

Табл. 4. Ил. 4. Библиогр.: 35 назв.

UDC 004.056.55

Substantiation and proposals for the selection, improvement and standardization of the post-quantum electronic signature mechanism at the national and international levels / *I.D. Gorbenko, O.G. Kachko, O.V. Potii,*

Yu.I. Gorbenko, V.A. Ponomar, M.V. Yesina, I.V. Stelnik, S.O. Kandiy, K.O. Kuznetsova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 5 – 26.

At present and in the future, mathematical methods, mechanisms and algorithms of standardized asymmetric cryptotransformations such as electronic signature (ES) are and will be used for information cryptographic protection. Electronic signature is the main and essential component of cybersecurity, in terms of providing quality information security services such as integrity, irresistibility and authenticity of information and data processed. However, there are well-founded suspicions that in the post-quantum period the existing ES standards will be broken and compromised using classical and quantum cryptanalytic systems with appropriate mathematical, software and hardware-software. An analysis was performed, which confirms that quantum computers have already been developed, manufactured and used. It is believed that the actual state of development and use of powerful quantum computers and their mathematical and software is obviously strictly confidential and secure, and only publicly known data on quantum computers and their applications in cryptology are disclosed. A preliminary analysis has been carried out showing that in Ukraine there is an understanding of the existence of threats to cybersecurity and information security in the case of using available standardized ES in the transition and post-quantum periods. Currently, development and adoption of post-quantum ES standards is also one of the main issues in ensuring the necessary levels of security in the transition and post-quantum periods. The objective of this article is to substantiate, compare alternatives and develop proposals for the selection and standardization of post-quantum ES standards at the international and national levels, taking into account the results of the 2nd and 3rd rounds of the NIST US competition and national researches.

Key words: electronic signature; information cryptographic protection; post-quantum period; «Сокіл»; Falcon; NIST PQC.

4 tab. 4 fig. Ref: 35 items.

УДК 004.056.5

Теоретичні основи формування ефективних кодових слів для стеганографічного методу з кодовим управлінням / *А.А. Кобозєва, А.В. Соколов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 27 – 39.

Стеганографія є важливою складовою сучасних систем захисту інформації. При цьому, в умовах сучасного кіберпростору, актуальною є розробка швидкодіючих стеганографічних методів, які мали б високий рівень стійкості до можливих атак стисненням, зашумленням і розмиттям. Одним з таких методів є стеганографічний метод з кодовим управлінням впровадження, заснований на ідеї попереднього додаткового кодування інформації, що впроваджуються за допомогою двійкових кодових слів, для яких трансформанти перетворення Уолша – Адамара мають задані властивості, що призводить до конкретної локалізації збурень в області перетворень Уолша – Адамара контейнера в результаті впровадження інформації. У роботі сформовано теоретичний базис для подальшого вдосконалення використовуваних у стеганографічному методі з кодовим управлінням кодових слів. Показано, що незважаючи на те, що зазначені кодові слова мають ідеальний вплив лише на задану трансформанту перетворення Уолша – Адамара, вони впливають відразу на кілька трансформант у просторі дискретного косинусного перетворення. Для вимірювання рівня вибірковості впливу на задану трансформанту дискретного косинусного перетворення (ДКП) введено поняття коефіцієнта селективності. Встановлено, що зі зростанням розміру блоків, що застосовуються, є тенденція до зменшення коефіцієнта селективності з огляду на наявність ефекту «близького сусіда». Ця тенденція, проте, обумовлена задіянням трансформант ДКП з близькими за значенням частотами, що мають подібну стійкість до можливих атак на впроваджене повідомлення. При цьому відношення суми модулів низькочастотних коефіцієнтів ДКП до суми модулів решти всіх коефіцієнтів ДКП зростає зі збільшенням розміру кодового слова. Доведено і практично підтверджено, що збільшення розміру кодового слова призводить до збільшення стійкості стеганографічного методу з кодовим управлінням. Теоретично обґрунтовано можливі способи подальшого практичного вдосконалення кодових слів, що застосовуються у стеганографічному методі з кодовим управлінням.

Ключові слова: стеганографія; дискретне косинусне перетворення; перетворення Уолша – Адамара; кодове управління впровадженням інформації; коефіцієнт селективності.

Табл. 3. Іл. 3. Бібліогр.: 27 назв.

УДК 004.056.5

Теоретические основы формирования эффективных кодовых слов для стеганографического метода с кодовым управлением / *А.А. Кобозева, А.В. Соколов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 27 – 39.

Стеганография является важной составляющей современных систем защиты информации. При этом в условиях современного киберпространства актуальной является разработка быстродействующих стеганографических методов, которые бы обладали высоким уровнем устойчивости к возможным атакам сжатием, зашумлением и размытием. Одним из таких методов является стеганографический метод с кодовым управлением внедрением, основанный на идее предварительного дополнительного кодирования внедряемой информации двоичными кодовыми словами, для которых трансформанты преобразования Уолша – Адамара имеют заданные свойства, что приводит к конкретной локализации возмущений в области преобразований Уолша – Адамара контейнера в результате внедрения информации. В работе сформирован теоретический базис для дальнейшего совер-

шенствования применяемых в стеганографическом методе с кодовым управлением кодовых слов. Показано, что, несмотря на то, что указанные кодовые слова имеют идеальное воздействие лишь на заданную трансформанту преобразования Уолша – Адамара, они воздействуют сразу на несколько трансформант в пространстве дискретного косинусного преобразования. Для измерения уровня выборочности воздействия на заданную трансформанту дискретного косинусного преобразования (ДКП) введено понятие коэффициента селективности. Установлено, что с ростом размера применяемых блоков имеется тенденция к уменьшению коэффициента селективности ввиду наличия эффекта «близкого соседа». Данная тенденция, тем не менее, обусловлена задействованием трансформант ДКП с близкими по значению частотами, имеющими сходную устойчивость к возможным атакам на встроенное сообщение. При этом отношение суммы модулей низкочастотных коэффициентов ДКП к сумме модулей всех остальных коэффициентов ДКП растет с увеличением размера кодового слова. Доказано и практически подтверждено, что увеличение размера кодового слова приводит к увеличению устойчивости стеганографического метода с кодовым управлением. Теоретически обоснованы возможные способы дальнейшего практического совершенствования кодовых слов, применяемых в стеганографическом методе с кодовым управлением.

Ключевые слова: стеганография; дискретное косинусное преобразование; преобразование Уолша – Адамара; кодовое управление внедрением информации; коэффициент селективности.

Табл. 3. Ил. 3. Библиогр.: 27 назв.

UDC 004.056.5

Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method / *A.A. Kobozeva, A.V. Sokolov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 27 – 39.

Steganography is an important component of modern information security systems. At the same time, in the conditions of modern cyberspace, it is relevant to develop high-performance steganographic methods that would have a high level of resistance to possible attacks by compression, noise, and blur. One of such methods is the steganographic method with code-controlled information embedding, based on the idea of preliminary coding of the information being embedded using binary codewords, for which the transformants of the Walsh-Hadamard transform have the specified properties. A specific localization of disturbances in the Walsh-Hadamard transform domain of the container takes place because of the information embedding. In this paper, a theoretical basis has been formed for further improvement of the codewords used in the code-controlled information embedding steganographic method. It is shown that despite the fact that these codewords have an ideal effect only on a given transformant of the Walsh-Hadamard transform, they affect several transformants at once in the domain of the discrete cosine transform (DCT). The concept of the selectivity coefficient is introduced to estimate the level of selectivity of the impact on a given DCT transformant. It has been established that with an increase in the size of the blocks used, a tendency is observed to a decrease in the selectivity coefficient due to the presence of the “close neighbor” effect. This trend is conditioned by the involvement of the DCT transformants with similar frequencies that have similar resistance to possible attacks on the embedded message. In this case, the ratio of the sum of absolute values of low-frequency DCT transformants to the sum of absolute values of all other DCT transformants increases with the size of the codeword. In this paper it has been proven and practically confirmed that an increase in the size of a codeword leads to an increase in the resistance of the code-controlled information embedding steganographic method. Possible ways of further practical improvement of codewords used in the code-controlled information embedding steganographic method are theoretically substantiated.

Key words: steganography; discrete cosine transform; Walsh-Hadamard transform; code-controlled information embedding; selectivity coefficient.

3 tab. 3 fig. Ref: 27 items.

УДК 621.391.15 : 519.7

Оцінка обчислювальної складності алгоритму CSIDH на суперсингулярних скручених і квадратичних кривих Едвардса / *А.В. Бессалов, О.В. Циганкова, С.В. Абрамов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 40 – 51.

Розглянуто властивості скручених і квадратичних суперсингулярних кривих Эдвардса, що утворюють пари квадратичного кручення з порядком $p+1$ над простим полем F_p. Приведена модифікація алгоритму CSIDH, побудованого на изогениях цих кривих замість традиційної арифметики кривих у формі Монтгомери. Розраховано і табульовано параметри цих двох класів суперсингулярних кривих Едвардса при $p = 239$, на ізогеніях яких наведено приклад реалізації алгоритму CSIDH як схеми неінтерактивного розподілу секрету на основі секретних і відкритих ключів Аліси та Боба. Показано, що послідовності параметрів $\pm d^{(i)}$ ланцюжків ізогеній відповідно для квадратичних та скручених суперсингулярних кривих Едвардса мають реверсний характер на періоді послідовності. Запропоновано рекурентний алгоритм обчислення координат точок, які створюють ядра ізогеній непарних степенів, розглянуто його реалізація в різних координатних системах. Дано порівняльний аналіз вартості обчислень параметру d' ізогенної кривої E' з застосуванням $(W:Z)$-координат Фарашахи – Хоссейні і класичних проєктивних координат $(X:Y:Z)$. Відзначено, що всі обчислення в алгоритмі

CSIDH, які необхідні для обчислення загального секрету d_{AB}, зводяться лише до обчислень параметру d' ізогенної кривої E' і виконуються польовими операціями та скалярним добутком точки. Обговорюється дискусійне питання про відмову від обчислення ізогенної функції $\phi(R)$ точки R кривої в алгоритмі CSIDH.

Ключові слова: крива в узагальненій формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; лізогенія; w-координати; квадратичний лишок; квадратичний не лишок.

Табл. 1. Бібліогр.: 17 назв.

УДК 621.391.15 : 519.7

Оценка вычислительной сложности алгоритма CSIDH на суперсингулярных скрученных и квадратичных кривых Эдвардса / *А.В. Бессалов, О.В. Цыганкова, С.В. Абрамов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 40 – 51.

Рассмотрены свойства скрученных и квадратичных суперсингулярных кривых Эдвардса, образующих пары квадратичного кручения с порядком $p+1$ над простым полем F_p. Приведена модификация алгоритма CSIDH, построенного на изогениях этих кривых взамен традиционной арифметики кривых в форме Монтгомери. Рассчитаны и табулированы параметры этих двух классов суперсингулярных кривых Эдвардса при $p = 239$, на изогениях которых приведен пример реализации алгоритме CSIDH как схемы неинтерактивного разделения секрета на основе секретных и открытых ключей Алисы и Боба. Показано, что последовательности параметров $\pm d^{(i)}$ цепочек изогений соответственно для квадратичных и скрученных суперсингулярных кривых Эдвардса имеют реверсный характер на периоде последовательности. Предложен рекуррентный алгоритм вычисления координат точек, образующих ядра изогений нечетных степеней, рассмотрена его реализация в различных координатных системах. Дан сравнительный анализ стоимости вычислений параметра d' изогенной кривой E' с использованием $(W:Z)$-координат Фарашахи – Хоссейни и классических проєктивных координат $(X:Y:Z)$. Отмечено, что все вычисления в алгоритме CSIDH, необходимые для вычисления общего секрета d_{AB}, сводятся лишь к вычислениям параметра d' изогенной кривой E' и выполняются полевыми операциями и скалярным произведением точки. Обсуждается дискуссионный вопрос об отказе от вычисления изогенной функции $\phi(R)$ точки R кривой в алгоритме CSIDH.

Ключевые слова: кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; изогения; w-координаты; квадратичный вычет; квадратичный невычет.

Табл. 1. Библиогр.: 17 назв.

UDC 621.391.15 : 519.7

Estimation of the computational cost of the CSIDH algorithm on supersingular twisted and quadratic Edwards curves / *A.V. Bessalov, O.V. Tsygankova, S.V. Abramov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 40 – 51.

The properties of twisted and quadratic supersingular Edwards curves that form pairs of quadratic torsion with order $p+1$ over a prime field F_p are considered. A modification of the CSIDH algorithm based on the isogenies of these curves instead of the traditional arithmetic of curves in the Montgomery form is presented. The parameters of these two classes of supersingular Edwards curves for $p = 239$ are calculated and tabulated. An example of the isogenies of these curves in the implementation of the CSIDH algorithm as a non-interactive secret sharing scheme based on the secret and public keys of Alice and Bob is given. It is shown that the sequences of parameters $\pm d^{(i)}$ of isogeny chains for quadratic and twisted supersingular Edwards curves, respectively, have a reverse nature on the period of the sequence. A recurrent algorithm for calculating the coordinates of points that form the kernels of isogenies of odd degrees is proposed, and its implementation in various coordinate systems is considered. A comparative analysis of the cost of calculating the parameter d' of the isogenic curve E' using the Farashakhi-Hosseini $(W:Z)$-coordinates and classical projective coordinates $(X:Y:Z)$ is given. It is noted that all calculations in the CSIDH algorithm necessary to calculate the shared secret d_{AB} are reduced only to the calculation of the isogenic curve E' parameter d' and are performed by field operations and the scalar multiplication of the point. The controversial issue of refusal to calculate the isogenic function $\phi(R)$ of a curve point R in the CSIDH algorithm is discussed.

Key words: curve in generalized Edwards form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curve order; point order; isomorphism; isogeny; w-coordinates; quadratic residue; quadratic non residue.

1 tab. Ref: 17 items.

УДК 004.043

Методи та засоби деанонімізації транзакцій в блокчейн / *В.В. Дубіна, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 52 – 58.

Наведено результати дослідження властивостей формування та обробки транзакцій в блокчейн системах, з метою виявлення існуючих перешкод на шляху досягнення безпечного функціонування мережі, обробки і передачі даних між користувачами та визначення можливих засобів деанонімізації транзакцій. Анонімність у мережі – одна з причин популярності криптовалют та широкого поширення технології блокчейн. Однак її наявність є основою виникнення нечесних транзакцій, злочинних дій шахраїв і атак на систему. Тому одними з найголовніших на сьогоднішній день залишаються питання забезпечення надійного зберігання інформації та можливості відстеження підозрілої активності і своєчасного захисту користувачів у блокчейн системах. В статті досліджено відомі методи для підвищення анонімності і збереженні конфіденційності у сучасних мережах, заснованих на принципах технології блокчейн, виникаючі загрози у зв'язку з їх використанням і можливі шляхи відстеження дій учасників системи. Наводиться порівняльна характеристика відомих інструментів відстеження і можливих засобів деанонімізації історії проведених транзакцій. В результаті дослідження запропоновано використання окремої платформи для аналізу мережі у реальному часі, виявлення загроз та їх своєчасного усунення, із можливістю візуалізації залежностей і побудови адресних графів в результаті відстеження всього ланцюжка транзакцій. Інструмент дозволяє реалізовувати пошук серед криптовалютних адрес, блоків, транзакцій та тегів, а також виявляти кластери, пов'язані з певною адресою. Система проводить аналіз мережі у реальному часі, щоб отримати уявлення про статистику. Особлива увага приділяється виявленню так званих аномалій, тобто ідентифікації тих транзакцій, які відхиляються від стандартних структур. Це дозволяє виявляти і відстежувати потенційно зловмисні дії на ранніх стадіях.

Ключові слова: Blockchain; транзакція; консенсус; анонімність; деанонімізація.

Іл. 4. Бібліогр.: 19 назв.

УДК 004.043

Методы и средства деанонимизации транзакций в блокчейн / *В.В. Дубина, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 52 – 58.

Приведены результаты исследования свойств формирования и обработки транзакций в блокчейн системах, с целью выявления существующих препятствий для достижения безопасного функционирования сети, обработки и передачи данных между пользователями и определения возможных средств деанонимизации транзакций. Анонимность в сети – одна из причин популярности криптовалют и широкого распространения технологии блокчейн. Однако ее наличие является основой возникновения нечестных транзакций, преступных действий мошенников и атак на систему. Поэтому одними из главных на сегодняшний день остаются вопросы обеспечения надежного хранения информации и возможности отслеживания подозрительной активности и своевременной защиты пользователей в блокчейн системах. В статье исследованы известные методы повышения анонимности и сохранения конфиденциальности в современных сетях, основанных на принципах технологии блокчейн, возникающие угрозы в связи с их использованием и возможные пути отслеживания действий участников системы. Проводится сравнительная характеристика известных инструментов отслеживания и возможных средств деанонимизации истории проведенных транзакций. В результате исследования предложено использование отдельной платформы для анализа сети в реальном времени, выявление угроз и их своевременного устранения, с возможностью визуализации зависимостей и построения адресных графов в результате отслеживания всей цепочки транзакций. Инструмент позволяет реализовывать поиск среди криптовалютных адресов, блоков, транзакций и тегов, а также выявлять кластеры, связанные с определенным адресом. Система проводит анализ сети в реальном времени, чтобы получить представление о статистике. Особое внимание уделяется выявлению так называемых аномалий, то есть идентификации транзакций, которые отклоняются от стандартных структур. Это позволяет выявлять и отслеживать потенциально злонамеренные действия на ранних стадиях.

Ключевые слова: Blockchain; транзакция; консенсус; анонимность; деанонимизация.

Ил. 4. Библиогр.: 19 назв.

UDC 004.043

Methods and means of deanonymization of transactions in blockchain / *V.V. Dubina, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 52 – 58.

This paper presents the results of a study of the properties of transactions formation and processing of in blockchain systems, aimed to identify existing barriers to the secure functioning of the network, processing and transmission of data between users, and to determine possible means of deanonymizing transactions. The anonymity of the network is one of the reasons for cryptocurrencies popularity and widespread use of blockchain technology. However, its presence is the basis for unscrupulous transactions, criminal actions of fraudsters and attacks on the system. Therefore, one of the main issues today is to ensure the reliable storage of information and the ability to track suspicious activity and timely protection of users in blockchain systems. The article examines known methods of increasing anonymity and maintaining confidentiality in modern networks based on the principles of blockchain technology, the threats arising from their use and the possible ways of tracking the actions of system participants. A comparative description of known tracking tools and possible means of de-anonymization of the history of completed transactions is given. As a result of the study, it was proposed to use a separate platform to analyze the network in real time, identify threats and their timely elimination, with the ability to visualize relationships and build address graphs as a result of tracking the entire chain of transactions. The tool makes it possible to implement a search among cryptocurrency addresses, blocks, transactions and tags, as well as to identify clusters associated with a particular address. The system analyzes the network in real time to gain insight into the statistics. Particular attention is paid to detecting so-called anomalies, i.e., the

identification of transactions that deviate from standard structures. This allows identifying and tracking potentially malicious activities at an early stage.

Key words: Blockchain; transaction; consensus; anonymity; deanonymization.

4 fig. Ref: 19 items.

УДК 003.026:004.056

Аналіз шляхів підвищення стійкості криптоалгоритмів на алгебраїчних решітках щодо часових атак / *О.Є. Петренко, О.С. Петренко, О.В. Сєвєрінов, О.І. Фєдюшин, А.В. Зубрич, Д.В. Щербина* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 59 – 65.

Метою статті є дослідження алгоритмів, стійкість яких базується на пошуку короткого вектору решітки, а також визначення стійких до часових атак параметрів цих алгоритмів. Розглядаються існуючі способи генерації ключів та вибір параметрів для криптографічних перетворень на алгебраїчних решітках стійких до часових атак. Зазначено, що рівномірний розподіл коефіцієнтів для генерації ключів алгоритму NTRU має певні недоліки, а саме: алгоритм NTRU має обмежене число параметрів, придатних до застосування в криптоперетвореннях, що пов'язано з вразливістю даного алгоритму до часових атак. З огляду на це, розглянуто можливість застосування дискретного нормального (Гаусівського) розподілу для утворення ключової пари, який дозволить запобігти чутливості алгоритму до часових атак. Даний спосіб генерації дискретного нормального розподілу вимагає перевірки відповідності вибірки властивостям нормального закону. Запропоновано застосування набору тестів SAGA. Вони дозволяють перевірити вибірки Гауса, які отримані за допомогою дискретного нормального розподілу. Результат перевірки показує, має чи ні вибірка властивості, що притаманні нормальному закону розподілу. Застосовуючи статистичні тести SAGA над поліномами криптографічних перетворень NTRU, було зроблено висновок, що дискретна Гаусівська вибірка дозволяє генерувати стійкі до часових атак параметри, використовуючи в якості середньоквадратичного відхилення норму або довжину короткого базису (вектору) решітки.

Ключові слова: алгебраїчні рещітки; дискретний нормальний розподіл; тести SAGA; часові атаки.

Табл. 5. Бібліогр.: 5 назв.

УДК 003.026:004.056

Анализ путей повышения стойкости криптоалгоритмов на алгебраических решётках до временных атак / *О.Е. Петренко, А.С. Петренко, А.В. Северинов, А.И. Федюшин, А.В. Зубрич, Д.В. Щербина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 59 – 65.

Целью статьи является исследование алгоритмов, стойкость которых базируется на поиске короткого вектора решетки, а также определение стойких к временным атакам параметров этих алгоритмов. Рассмотрены существующие способы генерации ключей и выбор параметров для криптографических преобразований на алгебраических решетках, стойких к временным атакам. Показано, что равномерное распределение коэффициентов для генерации ключей алгоритма NTRU имеет недостатки, а именно: ограниченное число параметров, пригодных для использования в криптопреобразованиях. Это связано с уязвимостью алгоритма временными атаками. Рассмотрена возможность использования дискретного нормального распределения для формирования ключевой пары, которое позволит противостоять восприимчивости временным атакам. Данный способ генерации требует проверки полученной выборки на соответствие свойствам нормального распределения. Предложено использование тестов SAGA. Они позволяют проверить выборки Гаусса, которые получены с помощью дискретного нормального распределения. Результат проверки показывает, имеет или нет выборка Гаусса свойства нормального распределения. Применяя тесты SAGA над полиномами криптографических преобразований NTRU, сделали вывод, что Гауссовская выборка позволяет генерировать стойкие к временным атакам параметры, используя в качестве среднеквадратического отклонения норму или длину короткого вектора решетки.

Ключевые слова: алгебраические решетки; дискретное нормальное распределение; тесты SAGA; временные атаки.

Табл. 5. Библиогр.: 5 назв.

UDC 003.026:004.056

Analysis of ways to increase stability of cryptographic algorithms on algebraic lattices against time attacks / *O.E. Petrenko, O.S. Petrenko, O.V. Sievierinov, O.I. Fiediushyn, A.V. Zubrych, D.V. Shcherbina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 59 – 65.

The aim of this work is to study the algorithms, the stability of which is based on the search for a short lattice vector, as well as to obtain time-resistant parameters of these algorithms. Existing methods for generating keys and choosing parameters for cryptographic transformations on algebraic lattices resistant to time attacks are considered. It is shown that the uniform distribution of coefficients for generating the NTRU algorithm keys has certain shortages, namely, a limited number of parameters suitable for use in cryptographical transformations. This is due to the vulnerability of this algorithm to time attacks. The possibility of using a discrete normal (Gaussian) distribution to form a key pair, which will prevent the sensitivity of the algorithm to time attacks, is considered. This method of generation requires checking the obtained sample for compliance with the properties of the normal distribution. The usage of SAGA tests has been proposed. They make it possible to check the Gaussian samples obtained using the discrete normal distribution. The verification result shows whether or not the sample has properties that are inherent in the normal distribution. The application of the SAGA statistical tests to the NTRU cryptographic transformation polynomials allowed us to

conclude that the discrete Gaussian sample makes it possible to generate time-resistant parameters using the norm or the length of the short basis (vector) of the lattice as the mean-square deviation.

Key words: algebraic lattices; discrete normal distribution; SAGA tests; time attacks.

5 tab. Ref: 5 items.

УДК 004.056.55

Аналіз стійкості ARX схем шифрування до інтегральної атаки та атаки нездійснених диференціалів / *В.І. Руженцев, О.І. Федюшин, С.А. Кохан* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 66 – 73.

Аналізуються поширені ARX (Addition-Rotation-XOR) алгоритми шифрування: Chacha, Speckey, Simon, Chaskey, Sparkle. Ці алгоритми використовують лише три операції: модульне додавання, XOR додавання та циклічний зсув. Розробляються 16-бітні зменшені моделі цих алгоритмів, обираються і розроблюються методи аналізу та виконується аналіз стійкості цих алгоритмів до найбільш ефективних атак: інтегральної атаки та атаки нездійснених диференціалів**.** За показником – кількість елементарних операцій, яка потрібна для отримання показників випадкової підстановки та відсутності нездійснених диференціалів й інтегралів – визначено найбільш ефективні ARX алгоритми. Такими стали Speckey, який оперує двома 8-бітовими підблоками та потребує 36 елементарних операцій, та Chaskey, який працює з чотирма 4-бітовими підблоками і потребує 72 елементарні операції. Якщо рахувати, що одна 8-бітова операція еквівалентна двом 4-бітовим, то ці схеми є рівними за обраним показником. Найгірші показники продемонстрували 8-бітова схема Simon та 4-бітова схема ChaCha, які потребують майже вдвічі більшої кількості операцій ніж кращі схеми. Також зроблено висновок про важливість використання не однієї, а декількох операцій XOR додавання з ключем для загальної криптографічної стійкості ARX алгоритмів.

Ключові слова: криптоаналіз; стійкість; ARX-алгоритм; модульне додавання; циклічний зсув; нездійснений диференціал; різність; інтегральний криптоаналіз; випадкова підстановка.

Табл. 11. Іл. 6. Бібліогр.: 7 назв.

УДК 004.056.55

Анализ стойкости ARX схем шифрования к интегральной атаке и атаке невыполнимых дифференциалов / *В.И. Руженцев, А.И. Федюшин, С.А. Кохан* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 66 – 73.

Анализируются распространенные ARX (Addition-Rotation-XOR) алгоритмы шифрования: Chacha, Speckey, Simon, Chaskey, Sparkle. Эти алгоритмы используют три основные операции: модульное сложение, XOR сложение и циклический сдвиг. Разрабатываются 16-битовые уменьшенные модели этих алгоритмов, выбираются и разрабатываются методы анализа и выполняется анализ стойкости этих алгоритмов к наиболее эффективным для этого класса алгоритмов атакам: интегральная атака и атака невыполнимых дифференциалов**.** По показателю – количество элементарных операций, которое необходимо для получения показателей случайной подстановки и отсутствия невыполнимых дифференциалов и интегралов – определены наиболее эффективные ARX алгоритмы. Такими стали Speckey, которая оперирует двумя 8-битовыми подблоками и требует 36 элементарных операций, и Chaskey, которая работает с четырьмя 4-битовыми подблоками и требует 72 элементарные операции. Если считать, что одна 8-битовая операция эквивалентна двум 4-битовым, то эти схемы получаются равными по выбранному показателю. Худшие показатели продемонстрировали 8-битовая схема Simon и 4-битовая схема ChaCha, которые требуют почти вдвое больше операций, чем лучшие схемы. Также сделан вывод о важности использования не одной, а нескольких операций XOR сложения с ключом для общей криптографической стойкости ARX алгоритмов.

Ключевые слова: криптоанализ; стойкость; ARX-алгоритм; модульное сложение; циклический сдвиг; невіполнимый дифференциал; разность; интегральный криптоанализ; случайная подстановка.

Табл. 11. Ил. 6. Библиогр.: 7 назв.

UDC 004.056.55

Analysis of ARX encryption schemes resistance to the integral attack and impracticable differentials attack / *V.I. Ruzhentsev, O.I. Fediushyn, S.A. Kokhan* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 66 – 73.

Common ARX (Addition-Rotation-XOR) encryption algorithms are analyzed. These algorithms are Chacha, Speckey, Simon, Chaskey, Sparkle. These algorithms use three basic operations: modular addition, XOR addition, and rotation. 16-bit reduced models of these algorithms are developed, methods of analysis are selected and developed, and the analysis of the resistance of these algorithms to the most effective attacks (integral attack and attack of impossible differentials) for this class of algorithms is performed. According to the selected indicator – the number of elementary operations that is necessary to obtain parameters of random substitution and the absence of impossible differentials and integrals – the most effective ARX algorithms are determined. These are Speckey, which operates on two 8-bit subblocks and requires 36 elementary operations, and Chaskey, which operates on four 4-bit subblocks and requires 72 elementary operations. If we assume that one 8-bit operation is equivalent to two 4-bit operations, then these schemes are equal in terms of the chosen indicator. The worst performers were the 8-bit Simon scheme and the 4-bit ChaCha scheme, which require almost twice as many operations as the best schemes. A conclusion was also made about the im-

portance of using not one, but several XOR operations of key addition for the overall cryptographic strength of ARX algorithms.

Key words: cryptanalysis; strength; ARX algorithm; modular addition; cyclic shift; impossible differential cryptanalysis; difference; integral cryptanalysis; random permutation.

11 tab. 6 fig. Ref: 7 items.

УДК 003.026:004.056

Сильні та слабкі сторони алгоритму на основі багатовимірних перетворень rainbow та його здатність блокувати атаки сторонніми каналами / *Д.В. Гармаш* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 74 – 77.

Розглядається аналіз сутності та можливості захисту постквантового криптографічного алгоритму Rainbow. Розглядаються основні властивості алгоритмів на основі багатовимірних квадратичних перетворень. Наведено математичні схеми та операції, які використовуються алгоритмом Rainbow. Оцінюється перспектива застосування алгоритмів на основі багатовимірних квадратичних перетворень у постквантовий час. Дається оцінка того, які ресурси та обчислювальна енергія необхідна для вдалого використання алгоритмів на основі багатовимірних квадратичних перетворень. Наведено основні позитивні сторони алгоритму та його слабкості. Наведено аналізи стосовно здатності захисту алгоритму від атаки сторонніми каналами.

Ключові слова: Rainbow; криптоаналіз; вразливість; мінранк; схема; алгоритм.

Бібліогр.: 8 назв.

УДК 003.026:004.056

Сильные и слабые стороны алгоритма на основе многоизмерных преобразований rainbow и его способность блокировать атаки сторонними каналами / *Д.В. Гармаш* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 74 – 77.

Рассматривается анализ сущности и возможности защиты постквантового криптографического алгоритма Rainbow. Рассматриваются главные характеристики алгоритмов на базе многомерных квадратических преобразований. Представлены математические схемы и операции, используемые алгоритмом Rainbow. Оценивается перспектива применения алгоритмов на основе многомерных квадратических преобразований в постквантовое время. Дана оценка того, какие ресурсы и вычислительная энергия необходимы для успешного использования алгоритмов на основе многомерных квадратических преобразований. Приведены основные положительные стороны алгоритма и их слабости. Приведены анализы способности защиты алгоритма от атаки посторонними каналами.

Ключевые слова: Rainbow; криптоанализ; уязвимость; минранк; схема; алгоритм.

Библиогр.: 8 назв.

UDC 003.026:004.056

Strengths and weaknesses of the algorithm based on multidimensional rainbow transformations and its ability to block attacks by third party channels / *D.V. Harmash* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 74 – 77.

The paper considers the analysis of the essence and possibilities to protect the Rainbow post-quantum cryptographic algorithm. The main properties of algorithms based on multidimensional quadratic transformations are considered. Mathematical schemes and operations used by the Rainbow algorithm are given. The perspective of using algorithms based on multidimensional quadratic transformations in post-quantum time is estimated. An estimate of what resources and computing energy are required for the successful use of algorithms based on multidimensional quadratic transformations is given. The main positive aspects of the algorithm and its weaknesses are outlined. Analyzes are given regarding the ability of the algorithm to protect against attack by third-party channels.

Key words: Rainbow; cryptanalysis; vulnerability; minrank; scheme; algorithm.

УДК 004.7:517.9

Один підхід до побудови індивідуальних математичних моделей захисту у бездротових сенсорних мережах / *Є. В. Котух, В. О. Любчак, О. П. Страх* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 78 –82.

Сучасний рівень розвитку техніки та технологій характеризується постійним розширенням різноманіття й складності механічних та керованих об’єктів, функціонування яких відбувається в неперервно-дискретному за часом режимі. Одним із таких об’єктів є процес поширення шкідливого програмного забезпечення у бездротових сенсорних мережах, постійне зростання тенденцій до яких обумовлене їх використанням як єдиного виду самоорганізованої мережі передачі даних з найменшою трудомісткістю та маловитратністю.

Концепція побудови сенсорних мереж остаточно не сформувалася. Тож вивчення певних властивостей таких мереж є дуже важливим як для вітчизняної, так і для світової науки. Більш того, для стратегічно важливих галузей країни, зокрема оборонної, захист бездротових сенсорних мереж є дуже важливою складовою.

Запропоновано нову модель поширення шкідливого програмного забезпечення, яка описується деякою крайовою задачею для імпульсної динамічної системи на часовій шкалі.

Ключові слова: бездротова сенсорна мережа; шкідливе програмне забезпечення; крайова задача.

Бібліогр.: 19 назв.

УДК 004.7:517.9

Один подход к построению индивидуальных математических моделей защиты в беспроводных сенсорных сетях / *Е. В. Котух, В. А. Любчак, А. П. Страх* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 78 –82.

Современный уровень развития техники и технологий характеризуется постоянным расширением разнообразия и сложности механических и управляемых объектов, функционирование которых происходит в непрерывно-дискретном по времени режиме. Одним из таких объектов является процесс распространения вредоносного программного обеспечения в беспроводных сенсорных сетях, постоянный рост тенденций к которому обусловлен их использованием как единого вида самоорганизованной сети передачи данных с наименьшей трудоемкостью и малозатратностью.

Концепция построения сенсорных сетей совсем не сформировалась. Поэтому изучение определенных свойств таких сетей очень важно как для отечественной, так и для мировой науки. Более того, для стратегически важных отраслей страны, в частности оборонной, защита беспроводных сенсорных сетей является очень важной составляющей.

Предложена новая модель распространения вредоносного программного обеспечения, которая описывается некоторой краевой задачей для импульсной динамической системы на временной шкале.

Ключевые слова: беспроводная сенсорная сеть; вредоносное программное обеспечение; краевая задача.

Библиогр.: 19 назв.

UDC 004.7:517.9

One approach to the design of individual mathematical models of security in wireless sensor networks / *Y.V. Kotukh, V.O. Lyubchak, O.P. Strakh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 78 –82

The current level of development of engineering and technology is characterized by a constant expansion of the variety and complexity of mechanical and controlled objects, the operation of which occurs in a continuous-discrete time mode. One of these objects is the process of spreading malicious software in wireless sensor networks, the constant growth of trends towards which is due to their use as a single type of self-organized data transmission network with the least labor intensity and low cost.

The concept of building sensor networks has not been formed at all. Therefore, the study of certain properties of such networks is very important for both domestic and world science. Moreover, for the strategically important sectors of the country, in particular defense, the protection of wireless sensor networks is a very important component.

A new model of malware distribution is proposed, which is described by some boundary value problem for an impulsive dynamical system on a time scale.

Key words: wireless sensor network; malware; boundary value problem.

Ref: 19 items.

РАДІОЛОКАЦІЯ І РАДІОНАВІГАЦІЯ
РАДИОЛОКАЦИЯ И РАДИОНАВИГАЦИЯ
RADIOLOCATION AND RADIONAVIGATION

УДК 004.89: 621.396

Оцінка ефективності обробки радіолокаційних зображень на основі інтелектуального аналізу процесів / *В.В. Жирнов, С.В. Солонська, І.Ю. Шубін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 83 – 88.

Наведено результати розробки методу автоматичного виявлення радіолокаційних відміток повітряних об’єктів та їх розпізнавання з обробкою реальних записів в оглядових РЛС. Актуальність цієї роботи полягає у створенні системи автоматичної обробки інформації для забезпечення ефективного виявлення корисних сигналів за рахунок накопичення сигнальної (енергетичної) та смислової інформації. Метод заснований на визначенні семантичних складових на етапі формування і аналізу символьної моделі сигнальних відміток від точкових і протяжних повітряних об’єктів. Сигнальна інформація визначається предикатною функцією процесних знань формування та аналізу символьної моделі пачки імпульсних сигналів від точкових рухомих літальних апаратів таких як літак, вертоліт, БПЛА, і від протяжних атмосферних утворень – ангел-луна, хмари та інші. В результаті семантичного аналізу символьних зображень сигнальних відміток отримано класифікаційні відмітні ознаки повітряних об’єктів. Досліджено семантичні складові алгоритму прийняття рішень, що схожі на алгоритми прийняття рішень оператором. У розробленому алгоритмі сигнальна інформація записується предикатної функцією на множині амплітуд імпульсів сигнальної позначки, які перевищили деяке порогові значення. Розпізнавання повітряних об'єктів проводиться шляхом вирішення розроблених рівнянь предикатних операцій. Верифікація розробленого методу проведена на реальних даних, отриманих на оглядовій РЛС сантиметрового діапазону (тривалість імпульсу 1 мкс, частота зондування 365 Гц, період огляду 10 с). На основі цих даних змодельовано типи характерних позначок радіолокаційних сигналів. За результатами експериментів усі вони правильно ідентифіковані.

Ключові слова: семантичний аналіз; радіолокаційний сигнал; ідентифікація; протяжні атмосферні утворення; повітряний об'єкт.

Іл. 2. Бібліогр.: 15 назв.

УДК 004.89: 621.396

Оценка эффективности обработки радиолокационных изображений на основе интеллектуального анализа процессов / *В.В. Жирнов, С.В. Солонская, И.Ю. Шубин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 83 – 88.

Приводятся результаты разработки метода и экспериментальных исследований системы автоматического обнаружения радиолокационных отметок воздушных объектов и их распознавания с обработкою реальных записей в обзорных РЛС. Актуальность этих работ заключается в создании алгоритма системы автоматической обработки радиолокационной информации для обеспечения эффективного обнаружения полезных сигналов за счет накопления сигнальной (энергетической) и смысловой информации. Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели сигнальных отметок от точечных и протяженных воздушных объектов. Сигнальная информация описывается предикатной функцией процессных знаний формирования и анализа символьной модели пачки импульсных сигналов от точечных подвижных летательных аппаратов таких, как самолет, вертолет, БПЛА, и от протяженных атмосферных образований – ангел-эхо, облака, тучи. В результате семантического анализа символьных изображений сигнальных отметок получены классификационные отличительные признаки воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений оператором. В разработанном алгоритме сигнальная информация описывается предикатной функцией на множестве амплитуд импульсов сигнальной отметки, превысивших некоторое пороговое значение. Распознавание воздушных объектов проводится путем решения разработанных уравнений предикатных операций. Верификация разработанного метода проведена на реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных отметок радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

Ключевые слова: семантический анализ; радиолокационный сигнал; идентификация; протяженные атмосферные образования; воздушный объект.

Ил. 2. Библиогр.: 15 назв.

UDC 004.89: 621.396

Evaluation of radar image processing efficiency based on intelligent analysis of processes / *V. Zhyrnov, S. Solonskaya, I. Shubin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 83 – 88.

The paper presents results of development of the method and experimental studies of the system for automatic detection of radar signals of aerial objects and their recognition with the processing of real records in surveillance radars. The relevance of this work consists in creation of algorithms for automatic information processing to ensure effective detection of useful signals due to accumulation of signal (energy) and semantic information. The method is based on the definition of semantic components at the stage of formation and analysis of the symbolic model of signals from point and extended air objects. Signal information is described by the predicate function of process knowledge of the formation and analysis of a symbolic model of a burst of impulse signals from point-like mobile aircraft such as an airplane, a helicopter, a UAV, and from extended atmospheric formations such as angel-echoes, clouds. As a result of semantic analysis of symbolic images of signal marks, classification distinctive features of air objects were obtained. The semantic components of the decision-making algorithm, similar to the decision-making algorithms used by the operator, have been investigated. In the developed algorithm, signal information is described by a predicate function on the set of signal mark pulse amplitudes that have exceeded a certain threshold value. Recognizing of aerial objects is carried out by solving the developed equations of predicate operations. The verification of the developed method was carried out on real data obtained on a survey radar of the centimeter range (pulse duration was 1 μs, probing frequency wass 365 Hz, survey period was 10 s). Based on these data, the types of characteristic marks of radar signals are modeled. According to the results of the experiments, they were all correctly identified.

Key words: semantic analysis; radar signal; identification; extended atmospheric formations; aerial object.

2 fig. Ref: 15 items.

УДК 007.51

Особливості управління завадостійкістю оглядової РЛС при її придушенні активними завадами та інформаційними впливами, що заважають / *В.М. Канцедал, А.А. Могила* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 89 – 101.

Розглядаються особливості управління цілепокладанням при забезпеченні інформаційної стійкості режимів зондування оглядової РЛС при її придушенні активними завадами та інформаційними впливами, що заважають. Подолання складності процесів цілепокладання, обґрунтованості та оперативності прийняття рішень при дефіциті часу на його прийняття пов'язані із забезпеченням системності процесів цілепокладання, підвищенням рівнів їх інтелектуалізації та формалізації. Це сприятиме наданню бажаних властивостей багатоцільовим стратегіям та ситуаційному закону управління процесами РЕЗ та координації дій, що синтезуються в ході конфлікту.

Особливості подолання складності вирішуваної проблеми пов'язані з системністю процесів цілепокладання, підвищенням їх рівнів інтелектуалізації та формалізації.

Підвищення рівня інтелектуалізації процесів цілепокладання забезпечується:

- декомпозицією загальної задачі цілепокладання на окремі більш прості підзадачі з ефективними рішеннями, які реалізуються у відповідних підсистемах САУуст (або базових об'єднаннях її функціональних елементів) на етапах інформаційного забезпечення, підготовки, прийняття та реалізації рішень на ієрархічних рівнях управління;

- когнітивним аналізом цілей та рефлексивним синтезом процесів цілепокладання з залученням можливостей спеціалізованої інтелектуальної системи підтримки прийняття рішень для посилення креативно-рефлексивних здібностей суб'єкта управління та підвищення рівня його професійних компетенцій;

– поєднанням універсальності етапів раціональних управління синтезом стратегії управління процесами РЕЗ зі специфікою конфліктних ситуацій, суб'єктністю, когнітивним та рефлексивним характером інтелектуального управління.

Представлені способи та засоби часткової формалізації процесів цілепокладання, коли структурування головної мети проводиться з урахуванням належності до стратегій внутрішнього та зовнішнього управлінь РЕЗ, декомпозиції двосторонньої динамічної моделі конфлікту між системами комплексу РЕП і РЛС, ієрархії рівнів управління, застосованих різних підходів до цілепокладання і кризисного управління в цілому, а також методів обґрунтування цілей, витрат ресурсів та і контролю якості досягнення поставлених цілей.

Ці особливості дозволяють суттєво знизити ступінь суб'єктивності керуючих рішень щодо цілепокладання, і домогтися їх обґрунтованості, повноти, несуперечності та узгодженості.

Ключові слова: система управління; конфліктна ситуація; невизначеність; стійкість; цілепокладання; прийняття рішень, радіоелектронний захист.

Іл. 1. Бібліогр.: 24 назв.

УДК 007.51

Особенности управления помехозащищенностью обзорной РЛС при ее подавлении активными помехами и мешающими информационными воздействиями / *В.М. Канцедал, А.А. Могила* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 89 – 101.

Рассматриваются особенности управления целеполаганием при обеспечении информационной устойчивости режимов зондирования обзорной РЛС при ее подавлении активными помехами и мешающими информационными воздействиями. Преодоление сложности процессов целеполагания, обоснованности и оперативности принятия решений при дефиците времени на его принятие связано с обеспечением системности процессов целеполагания, повышением уровней их интеллектуализации и формализации. Это будет способствовать приданию синтезируемым в ходе конфликта многоцелевым стратегиям и ситуационному закону управления процессами РЭЗ и координации действий желательных свойств.

Повышение уровня интеллектуализации процессов целеполагания обеспечивается:

- декомпозицией общей задачи целеполагания на отдельные более простые подзадачи с эффективными решениями, реализуемые в соответствующих подсистемах САУ$_{уст}$ (или базовых объединениях ее функциональных элементов) на этапах информационного обеспечения, подготовки, принятия и реализации решений на иерархических уровнях управления;

- когнитивным анализом целей и рефлексивным синтезом процессов целеполагания с привлечением возможностей специализированной интеллектуальной системы поддержки принятия решений для усиления креативно-рефлексивных способностей субъекта управления и повышения уровня его профессиональных компетенций;

- совмещением универсальности этапов рациональных управления синтезом стратегии управления процессами РЭЗ со спецификой конфликтных ситуаций, субъектностью, когнитивностью и рефлексивным характером интеллектуального управления.

Представлены способы и средства частичной формализации процессов целеполагания, когда структурирование главной цели производится с учетом принадлежности к стратегиям внутреннего и внешнего управлений РЭЗ, декомпозиции двусторонней динамической модели конфликта между системами комплекса РЭП и РЛС, иерархии уровней управления, применяемых различных подходов к целеполаганию в кризисном управлении, а также методов обоснования целей, затрат ресурсов и контроля качества достижения поставленных целей.

Эти особенности позволяют существенно снизить степень субъективности управляющих решений для целеполагания и добиться их обоснованности, полноты, непротиворечивости и согласованности.

Ключевые слова: **с**истема управления; конфликтная ситуация; неопределенность; устойчивость; целеполагание; принятие решений, радиоэлектронная защита.

Ил. 1. Библиогр.: 24 назв.

UDC 007.51

Specific features of immunity control of survey radar under its suppression by active interference and interfering information effects / *V.M. Kantsedal, A.A. Mogyla* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 89 – 101.

The features of goal-setting control while ensuring the information stability of the sounding modes of a surveillance radar when it is suppressed by active interference and interfering information influences are considered. Overcoming

the complexity of goal-setting processes, the validity and efficiency of decision-making with a shortage of time for its adoption is associated with insuring the consistency of goal-setting processes, increasing the levels of their intellectualization and formalization. This will contribute to imparting the desired properties, synthesized during the conflict, to the multipurpose strategies and the situational law of the control of the REP processes and the coordination of actions.

An increase in the level of intellectualization of goal-setting processes is ensured by:

- decomposition of the general goal-setting problem into separate, simpler subtasks with effective solutions, implemented in the corresponding subsystems of the ACS_{stab} (or basic associations of its functional elements) at stages of information support, preparation, adoption and implementation of the decision at the stages of hierarchical levels of management;
- cognitive analysis of goals and reflexive synthesis of goal-setting processes using the capabilities of a specialized intelligent decision support system to enhance the creative-reflexive abilities of the subject of management and increase the level of his professional competencies;
- combining the universality of the stages of rational management of the synthesis of the strategy for managing the REP processes with the specifics of conflict situations, subjectivity, cognition and reflexivity nature of intellectual control.

Methods and means for partial formalization of goal-setting processes are presented, when the structuring of the main goal is carried out taking into account belonging to the strategies of internal and external control of the REP, the decomposition of the two-sided dynamic model of the conflict between the systems of the RES complex and the radar, the hierarchy of management levels, various approaches applied to goal-setting in a crisis management, as well as methods of justifying goals, resource costs and control of achieving the goals.

These features can significantly reduce the degree of subjectivity of management for goal-setting and achieve their validity, completeness, consistency.

Key words: control system; conflict situation; uncertainty; stability; goal setting; decision making. electronic protection.

1 fig. Ref: 24 items.

УДК 621.396.96, 621.397.48:004.932.2

Комплексування інформаційних каналів систем виявлення та спостереження безпілотних літальних апаратів з позицій теорії статистичних рішень / *В.М. Карташов, В.О. Посошенко, В.І. Колісник, А.І. Капуста, М.В. Рибников, Є.В. Першин, В.О. Кізка* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 102 – 112.

Безпілотні літальні апарати (БПЛА) забезпечують виконання широкого спектру корисних для людства завдань, але, з іншого боку, вони представляють серйозну загрозу в господарській, військовій та інших областях діяльності людини. Труднощі спостереження БПЛА з використанням сучасних технічних засобів, а також їх відносно невисока вартість призводять до розширення сфери протиправних дій з використанням БПЛА. Тому захист різних об'єктів від БПЛА є серйозним науково-технічним завданням сучасності.

Оскільки можливості відомих методів виявлення БПЛА різні, то на практиці реалізується спільне використання систем різного виду з метою підвищення інформативності одержуваних даних шляхом сумісної (комплексної) їх обробки.

Число публікацій в даній області постійно збільшується, значна увага приділяється й інтегрованим системам, побудованим з використанням різних фізичних сенсорів. Однак ефективність функціонування мультисенсорних систем з комплексною обробкою вихідних сигналів каналів на практиці залишається недостатньою.

Стаття присвячена дослідженню методів синтезу нових більш ефективних алгоритмів комплексування радіолокаційних, акустичних, оптичних і інфрачервоних інформаційних каналів інтегральних систем виявлення та розпізнавання БПЛА, які виконуються з позицій статистичної теорії оптимізації радіосистем.

Такий підхід дозволяє синтезувати оптимальну (відповідно до обраного критерію якості) комплексну систему обробку інформації, що забезпечує отримання максимальної кількості інформації з векторного процесу, що спостерігається на входах інформаційних каналів. Показана можливість побудови оптимального детектора БПЛА з використанням пізньої стратегії об'єднання інформації на рівні рішень, прийнятих в окремих каналах системи.

Ключові слова: безпілотний літальний апарат; виявлення; спостереження; комплексування; радіолокаційна станція; інтегрована система; інформаційний канал; обробка сигналів.

Іл. 1. Бібліогр.: 23 назв.

УДК 621.396.96, 621.397.48:004.932.2

Комплексирование информационных каналов систем обнаружения и наблюдения беспилотных летательных аппаратов с позиций теории статистических решений / *В.М. Карташов, В.А. Посошенко, В.И. Колесник, А.И. Капуста, Н.В. Рыбников, Е.В. Першин, В.А. Кизка* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 102 – 112.

Беспилотные летательные аппараты (БПЛА) обеспечивают выполнение широкого спектра полезных для человечества задач, но, с другой стороны, они представляют серьезную угрозу в хозяйственной, военной и других областях деятельности человека. Трудности наблюдения БПЛА с использованием современных техниче-

ских средств, а также их относительно невысокая стоимость приводят к расширению сферы противоправных действий с использованием БПЛА. Поэтому защита различных объектов от БПЛА представляет собой серьёзную научно-техническую задачу современности.

Поскольку возможности известных методов обнаружения БПЛА различны, то на практике реализуется совместное использования систем различного вида с целью повышения информативности получаемых данных путем совместной (комплексной) их обработки.

Число публикаций в данной области постоянно увеличивается, значительное внимание уделяется и интегрированным системам, построенным с использованием различных физических сенсоров. Однако эффективность функционирования мультисенсорных систем с комплексной обработкой выходных сигналов каналов на практике остаётся недостаточной.

Статья посвящена исследованию методов синтеза новых более эффективных алгоритмов комплексирования радиолокационных, акустических, оптических и инфракрасных информационных каналов интегральных систем обнаружения и распознавания БПЛА, выполняемых с позиций статистической теории оптимизации радиосистем.

Такой подход позволяет синтезировать оптимальную (в соответствии с выбранным критерием качества) комплексную систему обработку информации, обеспечивающую получение максимального количества информации из векторного процесса, наблюдаемого на входах информационных каналов. Показана возможность построения оптимального обнаружителя БПЛА с использованием поздней стратегии объединения информации на уровне решений, принимаемых в отдельных каналах системы.

Ключевые слова: беспилотный летательный аппарат; обнаружение; наблюдение; комплексирование; радиолокационная станция; интегрированная система; информационный канал; обработка сигналов.

Ил. 1. Библиогр.: 23 назв.

UDC 621.396.96, 621.397.48:004.932.2

Complexing of information channels of UAV detection and observation systems from the statistic solutions theory standpoint / *V.M. Kartashov, V.O. Pososhenko, V.I. Kolisnyk, A.I. Kapusta, M.V. Rybnykov, I.V. Pershyn*, V.A. Kizka // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 102 – 112.

Currently, unmanned aerial vehicles (UAVs) provide a wide range of useful tasks for humanity, but, on the other hand, they pose a serious threat in economic, military and other areas of human activity. Difficulties in observing UAVs using modern technical means, as well as their relatively low cost, lead to an expansion of the scope of UAVs based illegal actions. Therefore, the protection of various objects against UAVs is a serious scientific and technical task of today.

Since the possibilities of the known methods of UAV detection are different, the joint use of systems of different types is realized in practice nowadays, in order to increase the informativeness of the obtained data by their joint (complex) processing.

The number of publications in this field is constantly increasing, and considerable attention is paid to integrated systems built on the basis of various physical sensors. However, the efficiency of multi-sensor systems with integrated processing of the output signals of the channels in practice remains insufficient.

This article is devoted to the study of methods for the synthesis of new, more efficient algorithms for complexing radar, acoustic, optical and infrared information channels of integrated UAV detection and recognition systems, which are performed from the standpoint of statistical theory of radio system optimization.

This approach allows synthesizing the optimal (according to the selected quality criterion) complex information processing system, which ensures obtaining the maximum amount of information from the vector process observed at the inputs of information channels. There shown the possibility of constructing an optimal UAV detector with the use of the late strategy of combining information at the level of decisions made in individual channels of the system.

Key words: unmanned aerial vehicle; detection; observation; integration; radar station; integrated system; information channel; signal processing.

1 fig. Ref: 23 items.

УДК 621.396.96, 621.397.48

Виявлення радіолокаційних сигналів, розсіяних на акустичних збуреннях, створюваних БПЛА / *В.М. Карташов, В.О. Посошенко, В.І. Колісник, І.С. Селезньов, Р.І. Бобнев, А.І. Капуста* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 113 – 122.

Розглянуто задачу радіолокаційного моніторингу БПЛА за його акустичним випромінюванням. Показано, що у низці практичних випадків такий підхід переважає спостереження радіолокаційними методами безпосередньо планера БПЛА. Відзначено, що радіосигнали, що розсіяно на акустичних пакетах від БПЛА, характеризуються невідомою заздалегідь комплексною огинаючою, що не дозволяє використовувати методи оптимальної фільтрації для їх виявлення та оцінювання. Показано, що для вирішення цих задач доцільно використовувати принцип накопичення на інтервалі спостереження приведеної до дисперсії шуму енергії вузькосмугового випадкового процесу, використовуючи статистичні відмінності шумових коливань і адаптивної суміші "сигнал плюс шум". Показано, що наведена оцінка енергії має або центральний, або нецентральний розподіл "хі-квадрат" з певним числом ступенів свободи та параметром нецентральності, який більше або дорівнює нулю. В результаті

порівняння поточного значення параметра нецентральності з пороговим значенням приймається рішення про наявність або відсутність на інтервалі спостереження корисного сигналу при мінімальній апріорній інформації про його параметри. Відзначено, що відомі вирази для диференційної щільності ймовірностей центрального та нецентрального розподілу "хі-квадрат" дозволяє отримати якісні оцінки пристрою виявлення, що синтезовано. Запропоновано практичну структурну схему цього пристрою з використанням обробки у квадратурних каналах коливань, що приймаються.

Ключові слова: акустичне випромінювання БПЛА; радіолокація акустичних пакетів; апріорна невизначеність; центральний розподіл "хі-квадрат"; нецентральний розподіл "хі-квадрат"; статистичне накопичення; енергетичний підхід; пороговий виявник.

Іл. 3. Бібліогр.: 35 назв.

УДК 621.396.96, 621.397.48

Обнаружение радиолокационных сигналов, рассеянных на акустических возмущениях, создаваемых БПЛА / *В.М. Карташов, В.А. Посошенко, В.И. Колесник, И.С. Селезнев, Р.И. Бобнев, А.И. Капуста* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 113 – 122.

Рассмотрена задача радиолокационного мониторинга БПЛА по его акустическому излучению. Показано, что в ряде практических случаев такой подход предпочтительней наблюдения радиолокационными методами непосредственно планера БПЛА. Отмечено, что радиосигналы, рассеянные на акустических пакетах от БПЛА, характеризуются неизвестной заранее комплексной огибающей, что не позволяет использовать методы оптимальной фильтрации для их обнаружения и оценивания. Показано, что для решения этих задач целесообразно использовать принцип накопления на интервале наблюдения приведенной к дисперсии шума энергии узкополосного случайного процесса, используя статистические различия шумовых колебаний и аддитивной смеси "сигнал плюс шум". Показано, что приведенная к шумам оценка энергии имеет либо центральное, либо нецентральное распределение "хи-квадрат" с определенным числом степеней свободы и параметром нецентральности, большим или равным нулю. В результате сравнения текущего значения параметра нецентральности с пороговым значением выносится решение о наличии или отсутствии на интервале наблюдения полезного сигнала при минимальной априорной информации о его параметрах. Отмечено, что известные выражения для дифференциальных плотностей вероятности центрального и нецентрального распределений "хи-квадрат" позволяют получить качественные оценки синтезированного обнаружителя. Предложена практическая структурная схема обнаружителя с использованием обработки принимаемых колебаний в квадратурных каналах.

Ключевые слова: акустическое излучение БПЛА; радиолокация акустических пакетов; априорная неопределенность; центральное распределение "хи-квадрат"; нецентральное распределение "хи-квадрат"; статистическое накопление; энергетический подход; пороговый обнаружитель.

Ил. 3. Библиогр.: 35 назв.

UDC 621.396.96, 621.397.48

Detection of radar signals scattered by acoustic disturbances generated by UAVs / *V.M. Kartashov, V.A. Pososhenko, V.I. Kolesnik, I.S. Seleznjov, R.I. Bobnev, A.I. Kapusta* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 113 – 122.

The problem of UAV radar monitoring by its acoustic radiation is considered. It is shown that in a number of practical cases such an approach is preferable to observation by radar methods directly from the UAV airframe. It is noted that the radio signals scattered by acoustic packets from the UAV are characterized by an unknown in advance complex envelope, which does not allow the use of optimal filtering methods for their detection and estimation. It is shown that to solve these problems, it is advisable to use the principle of accumulation over the observation interval of the energy of a narrow-band random process reduced to the noise dispersion, using the statistical differences between noise fluctuations and the additive "signal-plus-noise" mixture. It is shown that the energy estimate reduced to noise has either a central or an off-center "chi-square" distribution with a certain number of degrees of freedom and an off-center parameter greater than or equal to zero. As a result of comparing the current value of the no centrality parameter with the threshold value, a decision is made on the presence or absence of a useful signal in the observation interval with minimal a priori information about its parameters. It is noted that the well-known expressions for the differential probability densities of the central and non-central chi-square distributions allow one to obtain qualitative estimates of the synthesized detector. A practical structural diagram of a detector using processing of received oscillations in quadrature channels is proposed.

Key words: UAV acoustic radiation; radar acoustic packages; a priori uncertainty; central chi-square distribution; off-center chi-square distribution; statistical accumulation; energy approach; threshold detector.

3 fig. Ref: 35 items.

УДК 621.396.96

Оцінка відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору / *М.Г. Ткач* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 123 – 131.

Значну роль в інформаційному забезпеченні систем контролю повітряного простору і управління повітряним рухом відіграють вторинні радіолокаційні системи спостереження повітряного простору. Ці системи забез-

печують радіолокаційне спостереження за повітряними об'єктами, які обладнані літаковими відповідачами і забезпечують двосторонній зв'язок за каналами запиту та відповіді для передачі даних між наземними радіолокаційними станціями та повітряними об’єктами.

У роботі проведено оцінку відносної пропускної здатності літакових відповідачів вторинних радіолокаційних систем спостереження повітряного простору при дії в каналі запиту корельованих та некорельованих завад. Аналіз пропускної здатності літакового відповідача показує, що літаковий відповідач не досягає максимального завантаження, яке закладено в наявну систему ідентифікації при дії навмисних корельованих завад. Це вказує на неоптимальне визначення коефіцієнта завантаження літакового відповідача існуючої вторинної радіолокаційної системи. Неправильне визначення максимального завантаження літакового відповідача призводить до зниження завадостійкості як літакового відповідача, так і всієї вторинної радіолокаційної системи. При цьому слід зазначити, що зацікавлена сторона має можливість несанкціонованого використання літакового відповідача для отримання інформації або паралізації останнього при застосуванні завад потрібної інтенсивності.

Ключові слова: вторинна радіолокаційна система; система спостереження; повітряний простір; літаковий відповідач; відносна пропускна здатність; ідентифікація; сигнал запиту; сигнал відповіді; завада.

Іл. 3. Бібліогр.: 38 назв.

УДК 621.396.96

Оценка относительной пропускной способности самолетных ответчиков вторичных радиолокационных систем наблюдения воздушного пространства / *М.Г. Ткач* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 123 – 131.

Значительную роль в информационном обеспечении систем контроля воздушного пространства и управлении воздушным движением играют вторичные радиолокационные системы наблюдения воздушного пространства. Эти системы обеспечивают радиолокационное наблюдение за воздушными объектами, которые оборудованы самолетными ответчиками и обеспечивают двустороннюю связь по каналам запроса и ответа передачи данных между наземными радиолокационными станциями и воздушными объектами.

В работе проведена оценка относительной пропускной способности самолетных ответчиков вторичных радиолокационных систем наблюдения воздушного пространства при действии в канале запроса коррелированных и некоррелированных помех. Анализ пропускной способности самолетного ответчика показывает, что самолетный ответчик не достигает максимальной загрузки, заложенной в существующую систему идентификации при действии преднамеренных коррелированных помех. Это указывает на неоптимальное определение коэффициента загрузки самолетного ответчика существующей вторичной радиолокационной системы. Неправильное определение максимальной загрузки самолетного ответчика приводит к снижению помехоустойчивости как самолетного ответчика, так и всей вторичной радиолокационной системы. При этом следует отметить, что заинтересованная сторона имеет возможность несанкционированного использования самолетного ответчика для получения информации или парализации последнего при применении помех нужной интенсивности.

Ключевые слова: вторичная радиолокационная система; система наблюдения; воздушное пространство; самолетный ответчик; относительная пропускная способность; идентификация; сигнал запроса; сигнал ответа; помеха.

Ил. 3. Библиогр.: 38 назв.

UDC 621.396.96

Estimation of the relative throughput of aircraft transponders of secondary airspace surveillance radar systems / *M.G. Tkach* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 123 – 131.

Secondary radar systems for monitoring airspace play a significant role in the information support of airspace control systems and air traffic control. These systems provide radar surveillance of airborne objects equipped with aircraft transponders and provide two-way communication via data request and response channels between ground radar stations and airborne objects.

The paper assesses the relative throughput of aircraft transponders of secondary radar systems for monitoring airspace under the influence of correlated and uncorrelated interference in the request channel. The assessment of the throughput of the aircraft transponder shows that the aircraft transponder does not reach the maximum load included in the existing identification system under the influence of deliberate correlated interference. This indicates a sub-optimal determination of the aircraft transponder load factor of the existing secondary radar system. Incorrect determination of the maximum load of the aircraft transponder leads to a decrease in the noise immunity of both the aircraft transponder and the entire secondary radar system. At the same time, it should be noted that the interested party has the possibility of unauthorized use of an aircraft transponder to obtain information or paralyze the latter when applying interference of the required intensity.

Key words: secondary radar system; surveillance system; air space; aircraft transponder; relative throughput; identification; request signal; response signal; interference.

3 fig. Ref: 38 items.

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ
СИСТЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
SYSTEMS AND METHODS OF INFORMATION PROTECTION

УДК 621.37: 004.056.5

Використання нестаціонарних шумових завад для протидії пасивним радіозакладкам / *С.П. Сергієнко, В.Г. Крижановський,, Д.В. Чернов, Л.В. Загоруйко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 132– 138.

Використання шумових завад для протидії несанкціонованому зніманню інформації стало розповсюдженою практикою для захисту інформації. В останній час з'явилися публікації, в яких показано потенційну можливість використання шумових завад для знімання інформації пасивними радіопідслуховуючими пристроями. В особливості підвищується вразливість приміщень, які захищають від підслуховуючих пристроїв, якщо радіочастотне зашумлення включається в періоди часу, коли там ведуться конфіденційні перемовини. Використання енергії хвиль радіозашумлення для підслуховування робить такі пристрої непримітними для нелінійних радіолокаційних приладів пошуку радіопідслуховуючих пристроїв, якщо вони включаються тільки при дії шумових сигналів. В роботі показано, що використання нестаціонарного шуму дає можливість протидії несанкціонованому зніманню інформації. Аналіз ефективності нестаціонарного радіочастотного шуму проводився на моделі кореляційного приймача сигналу. Кореляційний приймач має найбільшу чутливість, і він більш ефективно працює з шумоподібними сигналами. В роботі показано, що для протидії несанкційного знімання інформації треба використовувати шум, амплітудно модульований випадковим сигналом, спектр якого співпадає зі спектром потенційного інформаційного сигналу. Накладання більш потужного модуляційного шуму на більш слабкий інформаційний сигнал робить неможливим передачу інформації. На прикладі зміни потужності монохроматичного сигналу при передачі радіозакладкой з використанням стационарного і нестаціонарного шумів показано, що завдяки параметричному перерозподілу енергії сигналу по спектру модуляції нестаціонарного шуму потужність монохроматичного сигналу зменшується більш ніж на 10 дБ порівняно з передачею такого ж сигналу стаціонарним шумом. На основі цих результатів можна зробити висновок, що використання для радіочастотного придушення нестаціонарних шумових сигналів робить неможливим використання сигналів радіочастотного придушення для роботи пасивних підслуховуючих пристроїв.

Ключові слова: пасивні радіопідслуховуючі пристрої; радіочастотне придушення; нестаціонарний шум; захист інформації.

Іл. 6. Бібліогр.: 15 назв.

УДК 621.37: 004.056.5

Использование нестационарных шумовых помех для противодействия пассивным радиозакладкам / *С.П. Сергиенко, В.Г. Крыжановский, Д.В. Чернов, Л.В. Загоруйко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 132 – 138.

Использование шумовых помех для противодействия несанкционированному съему информации стало распространенной практикой для защиты информации. В последнее время появились публикации, в которых показана потенциальная возможность использования шумовых помех для съема информации пассивными радиоподслушивающими устройствами. Особенно повышается уязвимость помещений, защищаемых от подслушивающих устройств, если радиочастотное зашумление включается в периоды времени, когда там ведутся конфиденциальные переговоры. Использование энергии волн радиозашумления для подслушивания делает такие устройства незаметными для нелинейных радиолокационных приборов поиска радиоподслушивающих устройств, если они включаются только при воздействии шумовых сигналов. В работе показано, что использование нестационарного шума создает возможность противодействию несанкционированному съему информации. Анализ эффективности нестационарного радиочастотного шума проводился на модели корреляционного приемника сигнала. Корреляционный приемник имеет наибольшую чувствительность, и он более эффективно работает с шумоподобными сигналами. В работе показано, что для противодействия несанкционированного съема информации надо использовать шум, амплитудно-модулированный случайным сигналом, спектр которого совпадает со спектром потенциального информационного сигнала. Наложение более мощного модуляционного шума на более слабый информационный сигнал делает невозможным передачу информации. На примере изменения мощности монохроматического сигнала при передаче радиозакладкой с использованием стационарного и нестационарного шумов показано, что благодаря параметрическому перераспределению энергии сигнала по спектру модуляции нестационарного шума, мощность монохроматического сигнала уменьшается более чем на 10 дБ по сравнению с передачей такого же сигнала стационарным шумом. На основе этих результатов можно сделать вывод, что использование для радиочастотного подавления нестационарными шумовыми сигналами делает невозможным использование сигналов радиочастотного подавления для работы пассивных подслушивающих устройств.

Ключевые слова: пассивные радиоподслушивающие устройства; радиочастотное подавления; нестационарный шум; защита информации.

Ил. 6. Библиогр.: 15 назв.

UDC 621.37: 004.056.5

The use of non-steady state noise interferences to counteract passive eavesdropping devices / *S.P. Serhiienko, V.G. Krizhanovski, D.V. Chernov, L.V. Zagoruiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 132 – 138.

The use of noise interference has become a common practice for information security. Recently appeared publications showing a potential possibility to use the noise radio frequency interference for information skimming by passive radio eavesdropping device. In particular, the vulnerability of the premises protected from eavesdropping devices is increased, if the radio frequency noising is switched on when confidential negotiations are being conducted. The use of radio noise waves energy for eavesdropping makes such devices invisible to nonlinear locators for listening devices if they activated only by noise signals. The paper shows that the use of non-steady state noise allows counteracting the unauthorized pickup of information. The analysis of non-steady state radio frequency noise effectiveness was carried out using the correlation receiver model. The correlation receiver has the highest sensitivity, and it works more efficiently with noise-like signals. It is shown that for counteracting the information pickup, it is necessary to use a noise, amplitude modulated by a random signal, whose spectrum coincides with a spectrum of a potential informational signal. Imposition a more powerful modulation noise to a weak informational signal makes impossible the information transfer. It is shown on the example of changing the power of a monochromatic signal while "beetle" transmits using steady-state and non-steady state noises, that due to the signal energy parametric redistribution over the non-steady-state noise modulation spectrum, the power of monochromatic signal is reduced by more than 10 dB compared to the transmission of the same signal using a steady-state noise. It can be concluded that the use of non-steady state noise signals for radio frequency suppression makes impossible their use for passive eavesdropping devices operation.

Key words: passive radio eavesdropping devices; radio-frequency suppression; non-steady state noise; information protection.

6 fig. Ref: 15 items.

УДК 621.369:534

Дослідження можливостей використання клавіатурного почерку для задач ідентифікації студентів у системах дистанційної освіти / *Д.Ю. Горєлов, О.О. Іванова, О.В Литвиненко, А.А. Довбня, Д.О. Мінін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 139 – 148.

В процесі використання систем дистанційної освіти виникає проблема інформаційної безпеки навчального процесу, яка, крім зовнішніх, містить також внутрішні загрози. Однією з таких загроз може стати легальний користувач, який заплатив шахраю за складання тестів та видимість навчальної діяльності під своїм ім'ям. Використання традиційних методів ідентифікації має два істотних недоліки: по-перше, неоднозначність користувача, який ідентифікується, оскільки в даному випадку встановлення особи користувача відбувається за введеною парольною фразою; по-друге, відсутність можливості виявлення підміни ідентифікованого користувача в процесі роботи з системою. Зазначені недоліки усуваються при використанні біометричних методів скритного та неперервного моніторингу.

У першій частині роботи проаналізовано типи тестових завдань. З урахуванням специфіки використання алгоритмів скритного клавіатурного моніторингу запропоновано: 1) використовувати тести, що не містять варіантів відповідей; 2) використовувати тести при поточному контролі знань з метою формування біометричного еталона користувача; 3) використовувати тести з числовими відповідями з метою мінімізації аналізованих дифрафів клавіатури.

У другій частині роботи запропоновано алгоритм формування профілю користувача та його ідентифікації, що поєднує якісний (розподіл частот використання груп цифрових клавіш, клавіш-розділювачів цілої та дробової частини, знаків «плюс» та «мінус» на основній та додатковій клавіатурах) та кількісний (аналіз статистичних властивостей диграфів) підходи. Експериментально отримані оцінки точності ідентифікації запропонованого алгоритму склали: FAR=4,64 % та FRR=6,25 %.

Ключові слова: інформаційна безпека систем дистанційної освіти; ідентифікація; клавіатурний почерк; диграф клавіатури; багатофакторна класифікація.

Табл. 2. Іл. 4. Бібліогр.: 16 назв.

УДК 621.369:534

Исследование возможностей использования клавиатурного почерка для задач идентификации студентов в системах дистанционного образования / *Д.Ю. Горелов, Е.А. Иванова, А.В Литвиненко, А.А. Довбня, Д.А. Минин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 139 – 148.

При использовании систем дистанционного образования возникает проблема информационной безопасности учебного процесса, которая, кроме внешних, подразумевает также и внутренние угрозы. Одной из таких угроз может стать легальный пользователь, который заплатил мошеннику за сдачу тестов и видимость учебной деятельности под своим именем. Использование традиционных методов идентификации имеет два существенных недостатка: во-первых, неоднозначность идентифицируемого пользователя, поскольку в данном случае установление личности пользователя происходит по введенной парольной фразе; во-вторых, отсутствие возможности обнаружения подмены идентифицированного пользователя в процессе работы с системой. Указанные недостатки устраняются при использовании биометрических методов скрытного и непрерывного мониторинга.

В первой части работы проанализированы типы тестовых заданий. С учетом специфики использования алгоритмов скрытного клавиатурного мониторинга предложено: 1) использовать тесты, не содержащие вариантов ответов; 2) использовать тесты при текущем контроле знаний с целью формирования биометрического эталона пользователя; 3) использовать тесты с численными ответами с целью минимизации анализируемых диграфов клавиатуры.

Во второй части работы предложен алгоритм формирования профиля пользователя и его идентификации, сочетающий качественный (распределение частот использования групп цифровых клавиш, клавиш-разделителей целой и дробной части, знаков «плюс» и «минус» на основной и дополнительной клавиатурах) и количественный (учет статистических свойств диграфов) подходы. Экспериментально полученные оценки точности идентификации предложенного алгоритма составили: FAR=4,64 % и FRR=6,25 %.

Ключевые слова: информационная безопасность систем дистанционного обучения; идентификация; клавиатурный почерк; диграф клавиатуры; многофакторная классификация.

Табл. 2. Ил. 4. Библиогр.: 16 назв.

UDC 621.369:534

Study of the possibilities to use keyboard handwriting for the tasks of identifying students in e-learning systems / *D.Y. Gorelov, O.O. Ivanova, O.V. Lytvynenko, A.A. Dovbnia, D.O. Minin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 139 – 148.

When using distance education systems, the problem of information security of the educational process arises, which, in addition to external ones, also implies internal threats. One of these threats can be a legitimate user who paid a fraudster to take tests and give visibility to educational activities under his own name. The use of traditional identification methods has two significant drawbacks: firstly, the ambiguity of the identified user, because the identification of the user occurs by the entered pair login-password; secondly, the inability to detect the substitution of an identified user in the process of working with the system. These disadvantages are eliminated by using biometric methods of covert and continuous monitoring.

In the first part of the work the different types of control knowledge tests are analyzed. Taking into account the specifics of the use of covert keyboard monitoring algorithms, the following is proposed: 1) to use tests that do not contain answers; 2) use tests after each learning activities in order to form a user's biometric vector; 3) use tests with numerical answers in order to minimize the analyzed keystroke digraphs.

An algorithm for user's profile formation and its identification is proposed in the second part of the work. Its combine qualitative (distribution of the frequencies of using numeric keys groups, comma-separated keys, "plus" and "minus" keys on the main and additional keyboard units) and quantitative (analysis of statistical properties of keystroke digraphs) approaches. The experimentally obtained estimates of the identification accuracy of the proposed algorithm: FAR=4.64% and FRR=6.25%.

Key words: information security of e-learning; authentication; keystroke; keystroke digraph; multi-factor classification.

2 tab. 4 fig. Ref: 16 items.

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ
ФИЗИКА ПРИБОРОВ, ЭЛЕМЕНТОВ И СИСТЕМ
PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

УДК 537.868

Вплив феримагнітного резонансу на перетворення енергії електромагнітної хвилі ЗІГ-резонатором в механічну енергію / *Г.Л. Комарова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 149 – 158.

Методом фізичного моделювання отриманий алгоритм обчислення сили, з якою стояча електромагнітна хвиля діє на феритову сферу довільного радіуса, розміщену в постійному магнітному полі. Величина напруженості постійного магнітного поля відповідає виникненню феримагнітного резонансу. Досліджено залежність магнітного поля електромагнітної хвилі в середині феритової сфери від розміру її резонансного радіусу і сферичних координат. У центрі феритової сфери, резонансний радіус якої дорівнює 4,2634 мм, напруженість магнітного поля НВЧ в 83796 разів більше в порівнянні з напруженістю магнітного поля в падаючій плоско поляризованій хвилі. Середнє квадратичне значення напруженості магнітного поля за обсягом кулі збільшується в 4,8 раз. Стояча електромагнітна хвиля, створена падаючою у вільному просторі з щільністю потоку потужності 622 кВт/м^2 і довжиною 3,2 см і відбитої від металевого екрана, розташованого від центру феритової сфери на відстані, рівній ($\lambda_o/8 + n \cdot \lambda_o/2$, де n = 0, 1, 2, 3 ...), діє на резонатор з силою, рівною 0,12 Н. Резонансний радіус феритової сфери дорівнює 4,2634 мм. Результати обчислень сили, діючої на ЗІГ-резонатор, збігаються з експериментальними результатами, наведеними в відомих роботах (щільність потоку потужності дорівнює 43 кВт / м2, радіус феритової сфери дорівнює 1,775 мм, сила дорівнює 6 ± 0,5 мкН) в межах похибки вимірювання. Застосування феримагнітного резонансу стоячої електромагнітної хвилі та ЗІГ-резонатора дозволило збільшити коефіцієнт перетворення енергії СВЧ в механічну в 8,6·10^4 разів у порівнянні з використанням фери-

тового циліндра в відомих роботах. Отримані результати можуть бути використані розробниками перетворювачів НВЧ енергії в механічну енергію.

Ключові слова: електромагнітна енергія; феримагнітний резонанс; перетворення; механічна енергія; ЗІГ-резонатор.

Табл. 1. Іл. 4. Бібліогр.: 14 назв.

УДК 537.868

Влияние ферримагнитного резонанса на преобразование энергии электромагнитной волны ЖИГ-резонатором в механическую энергию / *Г.Л. Комарова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 149 – 158.

Методом физического моделирования получен алгоритм вычисления силы, с которой стоячая электромагнитная волна действует на ферритовую сферу произвольного диаметра, помещенную в постоянное магнитное поле. Величина напряженности постоянного магнитного поля соответствует возникновению ферримагнитного резонанса. Исследованы зависимости магнитного поля электромагнитной волны в середине ферритовой сферы от размера ее резонансного радиуса и сферических координат. В центре ферритовой сферы, резонансный радиус которой равен 4,2634 мм, напряженности магнитного поля СВЧ в 83796 раз больше по сравнению с напряженностью магнитного поля в падающей плоскополяризованной волне. Среднее квадратичное значение напряженности магнитного поля по объему сферы увеличивается в 4,8 раз. Стоячая электромагнитная волна, созданная распространяющейся в свободном пространстве с плотностью потока мощности 622 кВт/м^2 и длиной 3,2 см и отраженной от металлического экрана, расположенного от центра ферритовой сферы на расстоянии, равном ($\lambda_o/8 + n\cdot\lambda_o/2$, где n = 0, 1, 2, 3…), действует на резонатор, с силой равной 0,12 Н. Резонансный радиус ферритовой сферы равен 4,2634 мм. Результаты вычисленный силы, действующей на ЖИГ-резонатор, совпадают с экспериментальными результатами, приведенными в известных работах (плотность потока мощности равна 43 кВт/м^2, радиус ферритовой сферы равен 1,775 мм, сила равна 6 ± 0,5 мкН) в пределах погрешности измерения. Применение ферримагнитного резонанса, стоячей электромагнитной волны и ЖИГ-резонатора позволило увеличить коэффициент преобразования энергии СВЧ в механическую энергию в $8{,}6\cdot10^4$ раз по сравнению с использованием ферримагнитного цилиндра в известных работах. Результаты исследований могут быть использованы разработчиками преобразователей СВЧ энергии в механическую энергию.

Ключевые слова: электромагнитная энергия; ферримагнитный резонанс; преобразование; механическая энергия; ЖИГ-резонатор.

Табл. 1. Ил. 4. Библиогр.: 14 назв.

UDC 537.868

Influence of ferrimagnetic resonance on conversion of electromagnetic energy by a YIG resonator into mechanical one / *G.L. Komarova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 149 – 158.

Using the method of physical modeling, an algorithm for calculating the force with which a standing electromagnetic wave acts on a ferrite sphere of arbitrary diameter placed in a constant magnetic field is obtained. The value of constant magnetic field intensity provides appearance of ferrimagnetic resonance. Dependence of the magnetic field of an electromagnetic wave in the middle of a ferrite sphere on the size of its resonant radius and spherical coordinates are studied. In the center of the ferrite sphere, the resonance radius of which is 4.2634 mm, the microwave magnetic field strength is 83796 times greater than the magnetic field strength in the incident plane polarized wave. Mean-square value of the magnetic field strength over the volume of the sphere increases 4.8 times. Standing wave, formed in a free space with power flow density of 622 kW/m^2 and wavelength of 3.2 cm, reflects from metallic shield placed at a distance of $\lambda_o/8 + n\lambda_o/2$, n = 0, 1, 2, 3… measured from the center of ferrite sphere and impacts with force of 0,12 N on ferrite sphere with resonance radius of 4,2634 mm. The results of the calculated force acting on the YIG – resonator coincide with the experimental results given in the well-known works (the power flux density is 43 kW/m^2, the radius of the ferrite sphere is 1.775 mm, the force is 6 ± 0.5 μN) within the measurement error. Application of spatial resonance, standing electromagnetic wave and YIG resonator allows to increase of energy conversion factor of microwave energy conversion into mechanic one $8{,}6\cdot10^4$ times in compare to application of ferrite cylinder only in known papers. The research results can be used by the developers of converters of microwave energy into mechanical energy.

Key words: electromagnetic energy; ferrimagnetic resonance; transformation; mechanical energy; YIG resonator.

1 tab. 4 fig. Ref: 14 items.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ
ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ТЕХНОЛОГИИ
INFORMATION AND MEASURING TECHNOLOGIES

УДК 004.45:004.057.02

Модель якості програмного забезпечення на основі стандартів SQuaRE / *Н.В. Штефан, О.В. Запорожець* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 159 – 165.

Якість є одним із факторів, що забезпечують комерційний успіх та безпеку використання програмного забезпечення. Під якістю розуміють відповідність явним і неявним вимогам різних зацікавлених сторін. Необхідно забезпечити спільне взаєморозуміння між розробниками та користувачами, інженери повинні розуміти зна-

чення поняття якості, характеристики та важливість якості для розробленого або підтримуваного програмного забезпечення. Основою забезпечення якості є вимірювання. Воно є основним інструментом керування життєвим циклом програмних продуктів, оцінки виконання планів і моніторингу. Для кількісного визначення якості необхідно виміряти характеристики програмного забезпечення. Стандартизація передбачає уніфікацію вимог до якості, її вимірювання та оцінки. Використання стандартів дає безліч потенційних переваг для будь-якої організації, особливо у таких ключових областях, як вимірювання якості програмних продуктів, інформаційних та вимірювальних систем. Визнані міжнародні організації із стандартизації опублікували серію стандартів ISO/IEC 25000 щодо вимог та оцінки якості систем та програмного забезпечення SQuaRE, які набувають широкого практичного застосування. У статті обговорюється серія міжнародних стандартів SQuaRE, аналізується взаємозв'язок між моделлю якості, характеристиками якості, показниками якості та новою концепцією – елементом показника якості програмного забезпечення, представлено вимірювання якості на основі цих стандартів.

Ключові слова: якість; модель якості; програмне забезпечення; вимірювання; стандарт; показник якості.

Табл. 1. Іл. 5. Бібліогр.: 10 назв.

УДК 004.45:004.057.02

Модель качества программного обеспечения на основе стандартов SQuaRE / *Н.В. Штефан, О.В. Запорожец* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 159 – 165.

Качество – один из основных факторов, обеспечивающих коммерческий успех и безопасность использования программного обеспечения. Качество понимается как соответствие явным и неявным требованиям различных заинтересованных сторон. Необходимо обеспечить совместное понимание между разработчиками и пользователями, инженеры должны понимать смысл, вкладываемый в концепцию качества, характеристики и значение качества в отношении разрабатываемого или сопровождаемого программного обеспечения. Основой обеспечения качества являются измерения. Они – основной инструмент управления жизненным циклом программных продуктов, оценки выполнения планов и мониторинга. Для количественного определения качества необходимо измерить характеристики программного обеспечения. Стандартизация обеспечивает унификацию требований к качеству, его измерению и оценке. Использование стандартов дает множество потенциальных преимуществ для любой организации, особенно в таких ключевых областях, как измерение качества программных продуктов, информационных и измерительных систем. Признанные международные организации по стандартизации опубликовали серию стандартов ISO/IEC 25000 по требованиям и оценке качества систем и программного обеспечения SQuaRE, которые получает все более широкое практическое применение. В статье рассмотрена серия международных стандартов SQuaRE, проанализировано отношение между моделью качества, характеристиками качества, показателями качества и новым понятием – элемент показателя качества программного обеспечения, представлено измерение качества на основе этих стандартов.

Ключевые слова: качество; модель качества; программное обеспечение; измерение; стандарт; показатель качества.

Табл. 1. Ил. 5. Библиогр.: 10 назв.

UDC 004.45:004.057.02

Software quality model based on SQuaRE standards / *N. Shtefan, O. Zaporozhets* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 159 – 165.

Quality is one of the factors that ensure the commercial success and safety of using the software. Quality is understood as conformity the explicit and implicit requirements of various stakeholders. It is necessary to ensure a joint understanding between developers and users, engineers need to understand the meaning of the concept of quality, characteristics and importance of quality for the developed or maintained software. Measurements are the basis for quality assurance. They are the main tool for managing the life cycle of software products, assessing the implementation of plans and monitoring. To quantify quality, it is necessary to measure the characteristics of the software. Standardization provides unification of requirements for quality, its measurement and assessment. The use of standards has many potential benefits for any organization, especially in key areas such as measuring the quality of software products, information and measurement systems. Recognized international standards organizations have published the ISO/IEC 25000 series of standards for systems and software quality requirements and evaluation SQuaRE, which is gaining widespread practical application. The paper discusses a series of international standards SQuaRE, analyzes the relationship between the quality model, quality characteristics, quality measures and a new concept – a quality measure element of the software, presents the measurement of quality based on these standards.

Key words: quality; quality model; software; measurement; standard; quality measure.

1 tab. 5 fig. Ref: 10 items.

СУМІЖНІ ПРОБЛЕМИ РАДІОТЕХНІКИ
СМЕЖНЫЕ ПРОБЛЕМЫ РАДИОТЕХНИКИ
RELATED PROBLEMS OF RADIO ENGINEERING

УДК 537.226.3

Оперативний контроль параметрів рідких паливомастильних матеріалів з домішками / *Б.В. Жуков, С.І. Борбулєв, А.В. Одновол* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2021. Вип. 207. С. 166 – 171.

Розглянуто можливості оперативного контролю параметрів рідких пально-мастильних матеріалів (ПММ) з домішками за допомогою резонаторного методу НВЧ діелектрометрії. Попередні дослідження рідких ПММ (бензини, дизельні палива, гаси, олії) показали, що величини дійсної та уявної складових комплексної діелектричної проникності перерахованих ПММ знаходяться в робочому діапазоні резонаторного НВЧ діелектрометра.

Висока роздільна здатність НВЧ резонаторного методу визначає перспективність використання даного методу для аналізу комплексної діелектричної проникності сумішей ПММ з різними домішками, включаючи воду, спирти, бензол та ін.

Для суміші бензину з бензолом експериментально встановлено, що при невеликій добавці бензолу (не більше 15 %) спостерігається зростання дійсної складової комплексної діелектричної проникності суміші, а при вмісті бензолу, що перевищує 15 %, має місце зростання обох складових комплексної діелектричної проникності суміші.

У процесі досліджень також було встановлено, що НВЧ діелектрометр забезпечив можливість ідентифікувати в реальному часі зразки трансформаторної олії за наявності води в кількості 14, 28 і 56 грам на тонну масла. Результати досліджень свідчать, що метод НВЧ діелектрометрії може вважатися перспективним для контролю якості трансформаторного масла як у процесі заливання, так і для контролю якості в процесі експлуатації високовольтних трансформаторів.

Результати початкового етапу досліджень спиртових бензинів поки що не дозволили виявити переважний вплив спиртової добавки на розташування експериментальних точок на комплексній площині. Ця обставина, найімовірніше, пов'язана з тим, що спиртові бензини з близьким октановим числом можуть мати хімічний склад, що істотно відрізняється.

Ключові слова: комплексна діелектрична проникність; НВЧ резонаторний метод; спиртовий бензин; масло трансформаторне; бензол; комплексна площина; октанове число.

Іл. 3. Бібліогр.: 17 назв.

УДК 537.226.3

Оперативный контроль параметров жидких горючесмазочных материалов с примесями / *Б.В. Жуков, С.И. Борбулев, А.В. Одновол* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 166 – 171.

Рассмотрены возможности оперативного контроля параметров жидких горючесмазочных материалов (ГСМ) с примесями с помощью резонаторного метода СВЧ диэлектрометрии. Предварительные исследования жидких ГСМ (бензины, дизельные топлива, керосины, масла) показали, что величины действительной и мнимой составляющих комплексной диэлектрической проницаемости перечисленных ГСМ находятся в рабочем диапазоне резонаторного СВЧ диэлектрометра.

Высокая разрешающая способность СВЧ резонаторного метода определяет перспективность использования данного метода для анализа комплексной диэлектрической проницаемости смесей ГСМ с различными примесями, включая воду, спирты, бензол и др.

Для смеси бензина с бензолом экспериментально установлено, что при небольшой добавке бензола (не более 15 %) наблюдается возрастание действительной составляющей комплексной диэлектрической проницаемости смеси, а при содержании бензола, превышающем 15 %, имеет место возрастание обеих составляющих комплексной диэлектрической проницаемости смеси.

В процессе исследований также было установлено, что СВЧ диэлектрометр обеспечил возможность идентифицировать в реальном времени образцы трансформаторного масла при наличии в них воды в количестве 14, 28 и 56 грамм на тонну масла. Результаты исследований свидетельствуют, что метод СВЧ диэлектрометрии может считаться перспективным для контроля качества трансформаторного масла как в процессе заливки, так и для контроля его качества в процессе эксплуатации высоковольтных трансформаторов.

Результаты начального этапа исследований спиртовых бензинов пока не позволили выявить преобладающее влияние спиртовой добавки на расположение экспериментальных точек на комплексной плоскости. Данное обстоятельство, вероятно, связано с тем, что спиртовые бензины с близким октановым числом могут иметь существенно отличающийся химический состав.

Ключевые слова: комплексная диэлектрическая проницаемость; СВЧ резонаторный метод; спиртовой бензин; масло трансформаторное; бензол; комплексная плоскость; октановое число.

Ил. 3. Библиогр.: 17 назв.

UDC 537.226.3

Operational control of the parameters of liquid fuels and lubricants with impurities / *B.V. Zhukov, S.I. Borbulev, A.V. Odnovol* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2021. №207. P. 166 – 171.

The possibilities of operational control of the parameters of liquid fuels and lubricants with impurities using the resonator method of microwave dielectrometry are considered. Preliminary studies of liquid fuels and lubricants (gasolines, diesel fuels, kerosene, oils) showed that the values of the real and imaginary components of the complex dielectric constant of the listed fuels and lubricants are in the operating range of the resonator microwave dielectrometer.

The high resolution of the microwave resonator method determines the prospects of using this method for analyzing the complex dielectric constant of mixtures of fuels and lubricants with various impurities, including water, alcohols, benzene, etc.

For a mixture of gasoline with benzene, it was experimentally established that with a small addition of benzene (no more than 15%), an increase in the real component of the complex dielectric constant of the mixture is observed, and with a benzene content exceeding 15%, an increase in both components of the complex dielectric constant of the mixture takes place.

The process has also been installed, but the NHF dielectrometer has made it possible to identify the transformer in real time due to the presence of water in the amount of 14, 28 and 56 grams per ton of oil. The research results indicate that the microwave dielectrometry method can be considered promising for monitoring the quality of transformer oil both during the filling process and for monitoring its quality during the operation of high-voltage transformers.

The results of the initial stage of research on alcohol gasolines have not yet revealed the predominant effect of the alcohol additive on the location of the experimental points on the complex plane. This circumstance is most likely due to the fact that alcohol gasolines with a close octane number can have a significantly different chemical composition.

Key words: complex dielectric constant; microwave resonator method; alcohol gasoline; transformer oil; benzene; complex plane; octane number.

3 fig. Ref: 17 items.