ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ
ПЕРСПЕКТИВНЫЕ МЕТОДЫ И СПОСОБЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ
PROSPECTIVE METHODS AND MEANS OF CRYPTOGRAPHIC TRANSFORMATIONS

УДК 004.056.55

Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / *І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 5 – 28.

На світовому рівні зусилля значного числа криптологів-теоретиків, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, Falcon та Rainbow. Окрім цього були визначені три альтернативні кандидати, які потребують більш детального дослідження. Всесторонній аналіз фіналістів є важливою задачею для криптологів світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів на стандарт ЕП – CRYSTALS-DILITHIUM та Falcon, ґрунтується на проблемах з теорії та практики алгебраїчних решіток. Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями". У статті розглядається сутність алгоритму ЕП CRYSTALS-DILITHIUM. Також проводиться детальний аналіз можливих атак на алгоритм та механізми їх реалізації. Розглядаються та аналізуються моделі порушника, загроз та безпеки. Надаються основні визначення щодо моделей безпеки ЕП. Описуються основні елементи конструкції механізму перспективного постквантового ЕП Dilithium в узагальненому вигляді. Наводяться загальні оцінки щодо рівня безпеки ЕП Dilithium. Приводиться обґрунтування та сутність моделей загроз, порушника та безпеки. Досліджується стійкість алгоритму ЕП Dilithium. Метою статті є обґрунтування моделі безпеки, класифікація, первинний аналіз та оцінка відомих атак на криптосистему ЕП CRYSTALS-DILITHIUM, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення 128, 256, 384 і 512 біт безпеки щодо класичного та 64, 128, 192 та 256 біт щодо квантового криптоаналізу.

Ключові слова: алгебраїчні решітки; атаки; безпека; загальносистемні параметри; модель безпеки; модель загроз; модель порушника; підпис; поліном; Dilithium.

Табл. 3. Іл. 1. Бібліогр.: 46 назв.

УДК 004.056.55

Методы вычисления системных параметров для электронной подписи «Crystals-Dilithium» 128, 256, 384 и 512 бит уровней безопасности / *И.Д. Горбенко, А.Н. Алексейчук, Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, С.А. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 5 – 28.

На мировом уровне усилия криптологов-теоретиков, математиков и криптологов-практиков сосредоточены на открытом конкурсе NIST PQC. Одной из основных задач конкурса является разработка и принятие постквантового или постквантовых стандартов ЭП. Финалистами второго этапа конкурса NIST стали три механизма ЭП – CRYSTALS-DILITHIUM, Falcon и Rainbow. Кроме этого были определены три альтернативных кандидата, которые требуют более детального исследования. Всесторонний анализ финалистов является важной задачей для криптологов мирового криптосообщества. Причем, безопасность, то есть доведение криптографической стойкости двух кандидатов-финалистов на стандарт ЭП – CRYSTALS-DILITHIUM и Falcon, основывается на проблемах по теории и практике алгебраических решеток. Метод (схема) ЭП Dilithium основывается на подходе, получившем название "Fiat-Shamir с прерываниями". В статье рассматривается суть алгоритма ЭП CRYSTALS-DILITHIUM. Также проводится детальный анализ возможных атак на алгоритм и механизмы их реализации. Даются основные определения относительно моделей безопасности ЭП. Описываются основные элементы конструкции механизма перспективного постквантового ЭП Dilithium в обобщенном виде. Приводятся общие оценки по уровню безопасности ЭП Dilithium. Приводится обоснование и сущность моделей угроз, нарушителя и безопасности. Исследуется стойкость алгоритма ЭП Dilithium. Цель статьи – обоснование модели безопасности, классификация, первичный анализ и оценка известных атак на криптосистему ЭП CRYSTALS-DILITHIUM, установление ограничений и разработка практических алгоритмов вычисления (генерации) общесистемных параметров для обеспечения 128, 256, 384 и 512 бит безопасности относительно классического и 64, 128, 192 и 256 бит относительно квантового криптоанализа.

Ключевые слова: алгебраические решетки; атаки; безопасность; общесистемные параметры; модель безопасности; модель угроз; модель нарушителя; подпись; полином; Dilithium.

Табл. 3. Ил. 1. Библиогр.: 46 назв.

UDC 004.056.55

Methods for calculating system parameters for electronic signature "Crystals-Dilithium" 128, 256, 384 and 512 bits of security levels / *I.D. Gorbenko, A.M. Aleksiychuk, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 5 – 28.

Globally, the efforts of a significant number of crypto-theorists, mathematicians and cryptologists-practitioners are focused on the NIST PQC open competition. One of the main tasks of the competition consists in development and adoption of a post-quantum ES standard or standards. The finalists of the second stage of the NIST competition were three ES mechanisms – CRYSTALS-DILITHIUM, Falcon and Rainbow. In addition, three alternative candidates were identified that require more detailed research. In general, a comprehensive analysis of the finalists is an important task for cryptologists in the global cryptocommunity. Moreover, security, i.e. bringing the cryptographic stability of two finalist candidates, to the ES standard – CRYSTALS-DILITHIUM and Falcon, is based on problems in the theory and practice of algebraic lattices. The EP Dilithium method (scheme) is based on the approach called "Fiat-Shamir Interruptions". The essence of the CRYSTALS-DILITHIUM ES algorithm is considered in the article. A detailed analysis of possible attacks on the algorithm and the mechanisms of their implementation is also carried out. Models of violator, threats and security are considered and analyzed. The main definitions of ES security models are provided. The main design elements of the mechanism of perspective post-quantum ES Dilithium are described in the generalized form. General estimations of the ES Dilithium security level are given. The substantiation and essence of models of threats, violator and security are given. The stability of the ES Dilithium algorithm is investigated. The purpose of the article is to substantiate a security model, classification, primary analysis and assessment of known attacks on the CRYSTALS-DILITHIUM EP cryptosystem, to establish restrictions and develop practical algorithms for calculating (generating) system-wide parameters to ensure 128, 256, 384 and 512 bits of security relative to classical and 64, 128, 192 and 256 bits relative to quantum cryptanalysis..

Key words: algebraic lattice; attacks; security; system-wide parameters; security model; threat model; violator model; signature; polynomial; Dilithium.

3 tab. 1 fig. Ref: 46 items.

УДК 004.056.55

Основні положення щодо моделі безпеки для асиметричних перетворень типу ЕП з урахуванням вимог та загроз постквантового періоду / *Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, М.В. Єсіна, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 29 – 36.

Наведено результати обґрунтування та розробка пропозицій щодо побудування моделі загроз щодо асиметричних криптоперетворень типу перспективний електронний підпис (ЕП), що може застосовуватись в постквантовий період. Викладено деталізовано узагальнені моделі загроз щодо перспективних ЕП та надається їх оцінка. Запропоновано моделі загроз щодо перспективних ЕП при застосуванні методів та засобів класичного та квантового криптоаналізу, моделі загроз при синтезі та застосуванні ЕП взагалі, а також моделі загроз при синтезі та застосуванні ЕП в постквантовий період. Формулюються пропозиції до переліку загроз, щодо яких повинен бути забезпечений захист. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП формується з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП, та застосуванні ЕП в постквантовий період. Розглядаються поняття EUF-CMA та SUF-CMA безпеки. Наводяться алгоритми роботи кожної із цих схем. Вводиться поняття комплексної моделі безпеки та наводяться її складові. Розглядається модель порушника та її суть. Наводяться основні загрози (атаки) із застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований та доступний для застосування). Наводяться та розглядаються атаки (загрози) стосовно перспективного ЕП. Проводиться аналіз схем підписів на відповідність необхідним моделям безпеки. Надаються основні поняття та визначення (поняття в термінології теорії ігор і т.д.). Вводяться та використовуються поняття «пряма секретність» та «досконала пряма секретність». Проводиться аналіз схем підпису, що є EUF-CMA та SUF-CMA безпечними. Розглядаються схеми підпису, що є залежними від ключів, з ключами, що розвиваються, з точки зору відповідності моделі безпеки EUF-CMA чи SUF-CMA. Також розглядається алгоритм підпису без стану. Наводяться алгоритми роботи таких схем підпису.

Ключові слова: асиметричний ЕП; класичний та квантовий криптоаналіз; модель загроз при синтезі ЕП; модель загроз при застосуванні ЕП; перелік загроз ЕП; постквантовий період.

Бібліогр.: 10 назв.

УДК 004.056.55

Основные положения по модели безопасности для асимметричных преобразований типа ЭП с учетом требований и угроз постквантового периода / *Ю.И. Горбенко, А.В. Потий, В.В. Ониприенко, М.В. Есина, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 29 – 36.

Приведены результаты, обоснование и разработка предложений по построению модели угроз относительно асимметричных криптопреобразования типа перспективная электронная подпись (ЭП), что может применяться в постквантовый период. Изложены обобщенные модели угроз по перспективным ЭП и дана их оценка. Предложены модели угроз по перспективным ЭП при применении методов и средств классического и квантового криптоанализа, модели угроз при синтезе и применении ЭП вообще, а также модели угроз при синтезе и применении ЭП в постквантовый период. Формулируются предложения по перечню угроз, в отношении которых должна быть обеспечена защита. Перечень возможных угроз безопасности применения существующих и

перспективных ЭП формируется из числа угроз, имеющихся в IT-Grundschutz Catalogues с учетом аппаратных, программных и аппаратно-программных ресурсов, технологий обработки данных и механизмов криптографической защиты при применении ЭП, в том числе с учетом требований и условий синтеза перспективных ЭП, и применении ЭП в постквантовый период. Рассматриваются понятие EUF-CMA и SUF-CMA безопасности. Приводятся алгоритмы работы каждой из этих схем. Вводится понятие комплексной модели безопасности и приводятся ее составляющие. Рассматривается модель нарушителя и его суть. Приводятся основные угрозы (атаки) с применением квантовых математических методов, которые могут быть реализованы на квантовом компьютере (конечно, если он будет построен и доступен для применения). Приводятся и рассматриваются атаки (угрозы) относительно перспективной ЭП. Проводится анализ схем подписей в соответствии с необходимыми моделями безопасности. Представляются основные понятия и определения (понятие в терминологии теории игр и т.д.). Вводятся и используются понятия «прямая секретность» и «совершенная прямая секретность». Проводится анализ схем подписи, которые являются EUF-CMA и SUF-CMA безопасными. Рассматриваются схемы подписи, которые являются зависимыми от ключей, с развивающимися ключами, с точки зрения соответствия модели безопасности EUF-CMA или SUF-CMA. Также рассматривается алгоритм подписи без состояния. Приводятся алгоритмы работы таких схем подписи.

Ключевые слова: асимметричная ЭП; классический и квантовый криптоанализ; модель угроз при синтезе ЭП; модель угроз при применении ЭП; перечень угроз ЭП; постквантовый период.

Библиогр.: 10 назв.

UDC 004.056.55

Basic statements on the security model for asymmetric transformations of the ES type taking into account the requirements and threats of the post-quantum period / *Yu.I. Gorbenko, O.V. Potii, V.V. Onoprienko, M.V. Yesina, G.A. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 29 – 36.

The paper presents the results of substantiation and development of proposals for building a threat model for asymmetric cryptotransformations such as a promising electronic signature (ES), which can be used in the post-quantum period. The generalized models of threats concerning perspective ES are stated in detail and their estimation is given. Threat models for promising ES using classical and quantum cryptanalysis methods and tools, threat models for synthesis and application of ES in general, as well as threat models for synthesis and application of ES in the post-quantum period are proposed. Proposals are formulated for a list of threats for which protection should be provided. The list of possible security threats to existing and future ES is formed from the number of threats available in IT-Grundschutz Catalogs, taking into account hardware, software and hardware-software resources, data processing technologies and cryptographic protection mechanisms in the use of ES, including requirements and conditions of synthesis of promising ES and application of ES in the post-quantum period. The concepts of EUF-CMA and SUF-CMA security are considered. Algorithms of work of each of these schemes are given. The concept of a comprehensive security model is introduced and its components are presented. The model of the violator and its essence are considered. The main threats (attacks) are given using quantum mathematical methods that can be implemented on a quantum computer (of course, if it is built and available for use). Attacks (threats) against a promising ES are presented and considered. The analysis of signature schemes for compliance with the required security models is performed. The terms "forward secrecy" and "perfect forward secrecy" are introduced and used. An analysis of signature schemes that are EUF-CMA and SUF-CMA secure is performed. Signature schemes, that are key-dependent, with evolving keys, are considered in terms of compliance with the EUF-CMA or SUF-CMA security model. The stateless signature algorithm is also considered. Algorithms of operation of such signature schemes are given.

Key words: asymmetric ES; classical and quantum cryptanalysis; model of threats in the synthesis of ES; model of threats in the use of ES; list of threats of ES; postquantum period.

Ref: 10 items.

УДК 004.056.55

Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері / *Є.Ю. Каптьол, І.Д. Горбенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 37 – 48.

Стаття присвячена деталізації можливостей та особливостей застосування квантового комп'ютера для програмування криптологічних задач, їх демонстрації, обгрунтуванню підходів до аналізу можливостей та вивчення особливостей програмування задач криптоаналізу на квантових комп'ютерах. Проаналізовано можливості та наявність забезпечення для вирішення задач криптоаналізу квантовими методами, а також визначено існуючі обмеження щодо їх використання. Розглянуто особливості та можливості квантового комп'ютера та програмування на квантовому комп'ютері. Також розглянуто можливості застосування квантового комп'ютера для криптоаналізу на прикладі методу Гровера. Наведено сутність методу Гровера та особливості його застосування для криптоаналізу. Наведено приклад його застосування для пошукового простору, що представлений квантовим регістром з 56 кубітів. Розглянуто застосування методу Гровера на квантовому комп'ютері, доступному через хмарний сервіс. Розроблено схеми проведення пошуку методом Гровера для застосування на квантовому комп'ютері, що містять різну кількість ітерацій Гровера для дослідження необхідності проведення повного циклу, можливості зупинки та оцінки результатів пошуку на певному етапі. Розроблені схеми перевірено на квантових комп'ютерах з різною архітектурою та на квантовому симуляторі, що наданий для аналізу схем, призна-

чених для запуску на квантовому комп'ютері. Наведено порівняння очікуваних та отриманих результатів застосування методу Гровера на різних етапах проведення пошуку на квантовому комп'ютері.

Ключові слова: квантовий комп'ютер; програмування на квантовому комп'ютері; метод Гровера; алгоритм Гровера; пошук несортованою базою даних; практичний приклад пошуку; приклади пошуку на квантовому комп'ютері.

Табл. 6. Іл. 5. Бібліогр.: 6 назв.

УДК 004.056.55

Анализ возможностей и особенностей программирования задач криптологии на квантовом компьютере / *Е.Ю. Каптел, И.Д. Горбенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 37 – 48.

Статья посвящена детализации возможностей и особенностей применения квантового компьютера для программирования криптологических задач, их демонстрации, обоснованию подходов к анализу возможностей и изучения особенностей программирования задач криптоанализа на квантовых компьютерах. Проанализированы возможности и наличие обеспечения для решения задач криптоанализа квантовыми методами, а также определены существующие ограничения по их использованию. Рассмотрены особенности и возможности квантового компьютера и программирования на квантовом компьютере. Также рассмотрены возможности применения квантового компьютера для криптоанализа на примере метода Гровера. Приведены суть метода Гровера и особенности его применения для криптоанализа. Также приведен пример его применения для поискового пространства, представленного квантовым регистром из 56 кубитов. Рассмотрено применение метода Гровера на квантовом компьютере, доступном через облачный сервис. Разработаны схемы проведения поиска методом Гровера для применения на квантовом компьютере, содержащие разное количество итераций Гровера для исследования необходимости проведения полного цикла, возможности остановки и оценки результатов поиска на определенном этапе. Разработанные схемы проверены на квантовых компьютерах с разной архитектурой и на квантовом симуляторе, предоставленном для анализа схем, предназначенных для запуска на квантовом компьютере. Приведено сравнение ожидаемых и полученных результатов применения метода Гровера на разных этапах проведения поиска на квантовом компьютере.

Ключевые слова: квантовый компьютер; программирование на квантовом компьютере; метод Гровера; алгоритм Гровера; поиск в несортированной базе данных; практический пример поиска; примеры поиска на квантовом компьютере.

Табл. 6. Ил. 5. Библиогр.: 6 назв.

UDC 004.056.55

Analysis of the possibilities and peculiarities of programming cryptology problems on a quantum computer / *Ye.Yu. Kaptol, I.D. Gorbenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 37 – 48.

This paper is devoted to detailing the possibilities and features of quantum computer use for cryptological problems, their demonstration, justification of approaches to the possibilities analysis and studying features of cryptanalysis problems programming on quantum computers. The possibilities and availability of hardware for solving cryptanalysis problems through quantum methods are analyzed and existing restrictions of their use are determined. The quantum computer and quantum computer programming features are considered. The possibilities of quantum computer use for cryptanalysis are also considered with the Grover's method example. The essence of Grover's method and features of its application for cryptanalysis are given. An example of its application to the search space which is represented by a quantum register of 56 qubits is given as well. The quantum computer application of Grover's method on quantum computer accessible through a loud service is considered. Schemes for conducting a search by Grover's method for quantum computer application are developed, containing a different number of Grover iterations to study the need for executing a full cycle, the possibility to stop and evaluate search results at a certain stage. The developed circuits are tested on quantum computers with different architectures and on a quantum simulator provided for the analysis of circuits intended to run on a quantum computer. The comparison of the expected and obtained results of the Grover's method application at different search stages on quantum computer is given.

Key words: quantum computer; quantum computer programming; Grover's method; Grover's algorithm; unsorted database search; practical search example; examples of search on a quantum computer.

6 tab. 5 fig. Ref: 6 items.

УДК 004.056.55

Аналіз стійкості постквантового електронного підпису Dilithium до атак на помилки / *Ю.І. Горбенко, О.С. Дроздова* // Радіотехника : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 49 – 56.

Проведено аналіз перспективного варіанту постквантового електронного підпису на основі алгебраїчних решіток Dilithium. Головною задачею аналізу є дослідження стійкості до атак на помилки, зокрема диференційних. Спочатку наводяться відомості про саму схему ЕП та її стійкість, атаки на помилки, їх розвиток до диференційних атак на помилки. Розглядаються можливості проведення цих атак та критерії їх успішного виконання. Було виявлено місця алгоритму ЕП, які потребують захисту від атак на помилки, такими є геш-функція (момент звернення та операція множення поліномів), етап завантаження особистого ключа, функція розширення початкового значення. Також повторне використання нонсу та часткове повторне використання нонсу при ге-

нерації ключів становить суттєву загрозу; провівши таку атаку, порушник може повністю відновити довгостроковий особистий ключ Dilithium. Сформовано заходи протидії на основі аналізу джерел, наведено їх переваги та негативні ефекти. Методами захисту від таких атак є: повторне обчислення підпису; перевірка підпису після підписання, що є втричі швидшим ніж попередній метод; внесення додаткової випадковості до детермінованої вибірки шуму; перевірка значення секретних та помилкових компонентів (нонсу); обчислення середнього значення та дисперсії вибірки, та їх перевірка на приналежність заданому діапазону. Результати роботи дають дослідникам орієнтир для розробки захищених схем постквантового електронного підпису.

Ключові слова: електронний підпис; постквантова криптографія; стійкість; диференційні атаки на помилки; заходи протидії.

Бібліогр.: 14 назв.

УДК 004.056.55

Анализ стойкости постквантовой электронной подписи Dilithium к атакам на ошибки / *Ю.И. Горбенко, О.С. Дроздова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 49 – 56.

Проведен анализ перспективного варианта постквантовой электронной подписи на основе алгебраических решеток Dilithium. Основной задачей анализа является исследование стойкости Dilithium к атакам на ошибки, в частности дифференциальных. Сначала приводятся сведения о самой схеме ЭП и ее стойкости, далее – атаки на ошибки и их развитие в дифференциальные атаки на ошибки. Рассматриваются возможности проведения этих атак и критерии их успешного выполнения. Были обнаружены места алгоритма ЭП, которые нуждаются в защите от атак на ошибки такие как, хеш-функция (момент обращения к ней и операция умножения полиномов), этап загрузки закрытого ключа, функция расширения начального значения. Также повторное использование нонсов и частичное повторное использование нонсов при генерации ключей составляет существенную угрозу, проведя такую атаку, нарушитель может полностью восстановить долгосрочный закрытый ключ Dilithium. Сформированны меры противодействия атакам на основе анализа источников, приведены их преимущества и побочные негативные эффекты. Методами защиты от таких атак являются: повторное вычисление подписи; проверка подписи после подписания, что в три раза быстрее чем предыдущий метод, внесение дополнительной случайности к детерминированной выборке шума; проверка значения секретных и ошибочных компонентов (нонсов) вычисления среднего значения и дисперсии выборки и их проверка на принадлежность заданному диапазону. Результаты работы дают исследователям ориентир для разработки защищенных схем постквантовой электронной подписи.

Ключевые слова: электронная подпись; постквантовая криптография; стойкость; дифференциальные атаки на ошибки; меры противодействия.

Библиогр.: 14 назв.

UDC 004.056.55

Analysis of Dilithium post-quantum electronic signature resistance to fault attacks / *U.I. Gorbenko, O.S. Drozdova* // // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 49 – 56.

Analysis of a perspective variant of post-quantum electronic signature based on algebraic lattices of Dilithium is carried out. The central task of the analysis is to study the resistance of Dilithium to fault attacks, in particular differential ones. First, information is given about the ES scheme itself and its security, fault attacks, their development to differential fault attacks. Possibilities of carrying out these attacks and criteria of their successful execution are considered. The places of the ES algorithm that need protection against fault attacks were identified, such as hash function (the moment of access to it and operation of polynomials multiplying), the stage of loading the private key, the function of expanding seed. Also, nonce reuse and partial nonce reuse when generating keys poses a significant threat, and by carrying out such an attack, the attacker can fully recover the long-term Dilithium private key. Attacks countermeasures are formed based on the sources analysis, their advantages and negative effects are presented. Methods of protection against such attacks are: re-calculation of the signature; verification of signature after signing, which is three times faster than the previous method; introducing additional randomness to the deterministic noise sampling; checking the value of secret and false components (nonce); calculating the average value and variance of the sample, and checking them for belonging to a given range. The results of this work provide researchers with a guide for the development of secure post-quantum electronic signature schemes.

Key words: electronic signature, post-quantum cryptography, security, differential fault attack, countermeasures.

Ref.: 14 items.

УДК 004.056.55

Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки / *І.Д. Горбенко, С.О. Кандій, М.В. Єсіна, Є.В. Острянська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 57 – 63.

На світовому рівні зусилля криптологів-теоретиків, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC. Одним із основних завдань конкурсу є розробка та прийняття постквантового чи постквантових стандартів ЕП. Фіналістами другого етапу конкурсу NIST стали три механізми ЕП – CRYSTALS-DILITHIUM, Falcon та Rainbow. Окрім цього, були визначені три альтернативні кандидати, які потребують більш детального дослідження. Всесторонній аналіз фіналістів є важливою задачею для криптологів

світової криптоспільноти. Причому, безпека, тобто доведення криптографічної стійкості двох кандидатів-фіналістів на стандарт ЕП – CRYSTALS-DILITHIUM та Falcon ґрунтується на проблемах з теорії та практики алгебраїчних решіток. Дослідження показують, що серед схем ЕП на решітках дещо відрізняється від інших кандидатів та має перспективи щодо прийняття в якості стандарту алгоритм Falcon. Основним та домінуючим підходом до проєктування механізму ЕП Falcon є використання перетворення Фіата – Шаміра з перериваннями. Для безпечного використання ЕП Falcon повинні бути знайдені набори загальносистемних параметрів, за яких забезпечується стійкість до всіх відомих та потенційних атак. В процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на думку авторів, на перспективу доцільним є забезпечення не менше 384 і 512 біт безпеки щодо класичного криптоаналізу та не менше 192 та 256 біт безпеки щодо квантового криптоаналізу. У статті коротко розглядається сутність алгоритму ЕП Falcon. Також проводиться аналіз можливих атак на алгоритм та механізми їх реалізації. Розглядається процес генерації загальносистемних параметрів для 256, 384, 512 біт стійкості. Наводяться висновки та рекомендації. Метою роботи є класифікація та первинний аналіз відомих атак на криптосистему ЕП Falcon, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для забезпечення не менше, ніж 256, 384 і 512 біт безпеки щодо класичного та не менше, ніж 128, 192 та 256 біт безпеки щодо квантового криптоаналізу.

Ключові слова: алгебраїчні решітки; атаки; безпека; загальносистемні параметри; підпис; поліном; Falcon.

Табл. 3. Бібліогр.: 12 назв.

УДК 004.056.55

Генерация общесистемных параметров для криптосистемы Falcon для 256, 384, 512 бит безопасности / *И.Д. Горбенко, С.А. Кандий, М.В. Есина, Е.В. Острянская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 57 – 63.

На мировом уровне усилия криптологов-теоретиков, математиков и криптологов-практиков сосредоточены на открытом конкурсе NIST PQC. Одной из основных задач конкурса является разработка и принятие постквантового или постквантовых стандартов ЭП. Финалистами второго этапа конкурса NIST стали три механизма ЭП – CRYSTALS-DILITHIUM, Falcon и Rainbow. Кроме этого, были определены три альтернативных кандидата, которые требуют более детального исследования. В целом всесторонний анализ финалистов является важной задачей для криптологов мирового криптосообщества. Причем, безопасность, то есть доведение криптографической стойкости двух кандидатов-финалистов, на стандарт ЭП – CRYSTALS-DILITHIUM и Falcon, основывается на проблемах по теории и практике алгебраических решеток. Исследования показывают, что среди схем ЭП на решетках несколько отличается от других кандидатов и имеет перспективы для принятия в качестве стандарта алгоритм Falcon. Основным и доминирующим подходом к проектированию механизма ЭП Falcon является использование преобразования Фиата – Шамира с прерываниями. Для безопасного использования ЭП Falcon должны быть найдены наборы общесистемных параметров, при которых обеспечивается устойчивость ко всем известным и потенциальным атакам. В процессе формирования требований к ЭП NIST в рамках конкурса был заинтересован только в наборах общесистемных параметров до 256 бит классической безопасности включительно. Однако, по мнению авторов, на перспективу целесообразно обеспечить не менее 384 и 512 бит безопасности по классическому криптоанализу и не менее 192 и 256 бит безопасности – по квантовому криптоанализу. В статье кратко рассматривается сущность алгоритма ЭП Falcon. Также проводится анализ возможных атак на алгоритм и механизмы их реализации. Рассматривается процесс генерации общесистемных параметров для 256, 384, 512 бит стойкости. Приводятся выводы и рекомендации. Цель работы – классификация и первичный анализ известных атак на криптосистему ЭП Falcon, установление ограничений и разработка практических алгоритмов вычисления (генерации) общесистемных параметров для обеспечения не менее 256, 384 и 512 бит безопасности относительно классического и не менее 128, 192 и 256 бит безопасности относительно квантового криптоанализа.

Ключевые слова: алгебраические решетки; атаки; безопасность; общесистемные параметры; подпись; полином; Falcon.

Табл. 3. Библиогр.: 12 назв.

UDC 004.056.55

Generation of system-wide parameters for Falcon cryptosystem for 256, 384, 512 bits of security / *I.D. Gorbenko, S.O. Kandiy, M.V. Yesina, E.V. Ostryanska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 57 – 63.

Globally, the efforts of a significant number of crypto-theorists, mathematicians and cryptologists-practitioners are focused on the NIST PQC open competition. One of the main tasks of the competition consists in development and adoption of a post-quantum ES standard or standards. The finalists of the second stage of the NIST competition were three ES mechanisms – CRYSTALS-DILITHIUM, Falcon and Rainbow. In addition, three alternative candidates were identified that require more detailed research. In general, a comprehensive analysis of the finalists is an important task for cryptologists in the global cryptocommunity. Moreover, security, i.e. brining the cryptographic stability of two finalist candidates, to the ES standard – CRYSTALS-DILITHIUM and Falcon, is based on problems in the theory and practice of algebraic lattices. Studies show that among the ES schemes on lattices it differs slightly from other candidates and has prospects for the adoption as the Falcon algorithm standard. The main and dominant approach to the design of the Falcon ES mechanism is the use of the Fiat-Shamir transformation with interruptions. The sets of system-wide pa-

rameters that ensure resistance to all known and potential attacks should be found for the safe use of the Falcon ES. In the process of forming the requirements for ES within the competition, the NIST was interested only in sets of system-wide parameters up to 256 bits of classical security inclusive. However, according to the authors of this work, in the future it is advisable to provide at least 384 and 512 bits of security for classical cryptanalysis and at least 192 and 256 bits of security for quantum cryptanalysis. The article briefly considers the essence of the Falcon electronic signature (ES) algorithm. An analysis of possible attacks on the algorithm and the mechanisms of their implementation is also performed. The process of generating system-wide parameters for 256, 384, 512 stability bits is considered. Conclusions and recommendations are given. The objective of the work is the classification and initial analysis of known attacks on the ES Falcon cryptosystem, setting limits and developing practical algorithms for calculating (generating) system-wide parameters to provide not less than 256, 384 and 512 security bits for classical and not less than 128, 192 and 256 security bits for quantum cryptanalysis.

Key words: algebraic lattice; attacks; security; system-wide parameters; signature; polynomial; Falcon.
3 tab. Ref: 12 items.

УДК 004.056.55

Процеси та методи вибору загальносистемних параметрів перспективного алгоритму електронного підпису на основі алгебраїчних решіток / *В.А Кулібаба* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 64 – 71.

Важливою особливістю перехідного та постквантового періоду є застосування нових математичних методів для протидії квантовому криптоаналізу. Особливу увагу світове криптографічне співтовариство приділяє відкритому конкурсу на постквантовий стандарт електронного підпису. Проблемним питанням є доведення стійкості нових математичних методів синтезу перетворень типу електронний підпис, зокрема з використанням алгебраїчних решіток. Проаналізовано існуючі алгоритми електронного підпису 2-го етапу конкурсу NIST. Серед обраних кандидатів на стандарт ЕП два із трьох алгоритмів засновані на алгебраїчних решітках, це CRYSTALS-DILITHIUM та FALCON. NIST випустив заяву про те, що скоріше за все буде обрано один із алгоритмів через однакому математичну базу, що застосовується в обох алгоритмах. Розглядаються основні атаки на алгоритми електронного підпису, засновані на проблемі навчання з помилками, а також параметри алгоритму ЕП Dilithium, що впливають на стійкість та складність перетворень. Розглядаються методи генерування загальносистемних параметрів рівнів стійкості 512 біт класичної та 256 біт квантової безпеки, а також захищеність алгоритму від атак сторонніми каналами. Проаналізовано залежність часу вироблення електронного підпису від ключів. Подано результати обчислень параметрів для рівня стійкості 512/256, а також надано рекомендації щодо вибору загальносистемних параметрів. Розглянуто результати 2-го етапу конкурсу постквантових криптоалгоритмів NIST, а також перспективи стандартизації перетворень типу електронний підпис на 3-му етапі. Зроблено висновки про необхідність більш детального вивчення атак на алгоритми, засновані на проблемі навчання з помилками, а також про важливість генерування загальносистемних параметрів більш високих порядків.

Ключові слова: загальносистемні параметри; алгоритми постквантового електронного підпису; алгебраїчні решітки; функції хешування; криптографічна стійкість.
Табл. 4. Іл. 1. Бібліогр.: 15 назв.

УДК 004.056.55

Процессы и методы выбора общесистемных параметров перспективного алгоритма электронной подписи на основе алгебраических решеток / *В.А Кулибаба* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 64 – 71.

Важной особенностью переходного и постквантового периода является применение новых математических методов для противодействия квантовому криптоанализу. Особое внимание мировое криптографическое сообщество уделяет открытому конкурсу на постквантовый стандарт электронной подписи. Проблемным вопросом является доказательство стойкости новых математических методов синтеза преобразований типа электронной подписи, в том числе с использованием алгебраических решеток. Проанализированы существующие алгоритмы электронной подписи 2-го этапа конкурса NIST. Среди выбранных кандидатов на стандарт ЭП два из трех алгоритмов основаны на алгебраических решетках, это CRYSTALS-DILITHIUM и FALCON. NIST выпустил заявление о том, что, скорее всего, будет выбран один из алгоритмов ввиду одинаковой математической базы, которая применяется в обоих алгоритмах. Рассматриваются основные атаки на алгоритмы электронной подписи, основанные на проблеме обучения с ошибками, а также параметры алгоритма ЭП Dilithium, влияющие на стойкость и сложность преобразований. Рассматриваются методы генерирования общесистемных параметров уровней стойкости 512 бит классической и 256 бит квантовой безопасности, а также защищенность алгоритма от атак посторонними каналами. Проанализирована зависимость времени генерации электронной подписи от ключей. Представлены результаты вычислений параметров для уровня стойкости 512/256, а также даны рекомендации по выбору общесистемных параметров. Рассмотрены результаты 2-го этапа конкурса постквантовых криптоалгоритмов NIST, а также перспективы стандартизации преобразований типа электронной подписи на 3-м этапе. Сделаны выводы о необходимости более детального изучения атак на алгоритмы, основанные

на проблеме обучения с ошибками, а также о важности генерирования общесистемных параметров более высоких порядков.

Ключевые слова: общесистемные параметры; алгоритмы постквантового электронной подписи; алгебраические решетки; функции хеширования; криптографическая стойкость.

Табл. 4. Ил. 1. Библиогр.: 15 назв.

UDC 004.056.55

Processes and methods of selection of system-wide parameters of perspective algorithm of electronic signature based on algebraic lattices / *V.A. Kulibaba* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 64 – 71.

An important feature of the transition and post-quantum period is the application of new mathematical methods to counteract quantum cryptanalysis. The world cryptographic community pays special attention to the open competition for the post-quantum standard of electronic signature. The problem is to prove the stability of new mathematical methods for the synthesis of transformations such as electronic signature, in particular with the use of algebraic lattices. The existing algorithms of electronic signature of the 2nd stage of the NIST competition are analyzed. Among the selected candidates for the EP 2 standard, 3 of the 3 algorithms are based on algebraic lattices, CRYSTALS-DILITHIUM and FALCON. The NIST has issued a statement saying that it is most likely that one of the algorithms will be chosen due to the same mathematical basis used in both algorithms. The main attacks on electronic signature algorithms based on the problem of learning with errors, as well as the parameters of the EP Dilithium algorithm, which affect the stability and complexity of transformations, are considered. Methods for generating system-wide parameters of stability levels of 512 bits of classical and 256 bits of quantum security, as well as the protection of the algorithm againstfrom attacks by third-party channels are considered. The dependence of the time of electronic signature production on the keys is analyzed. The results of calculations for the level of stability 512/256 are given, and also recommendations on the choice of system-wide parameters are given. The results of the 2nd stage of the NIST competition of post quantum cryptographic algorithms, as well as the prospects of standardization of transformations such as electronic signature at the 3rd stage are considered. Conclusions are made about the need for a more detailed study of attacks on algorithms based on the problem of learning with errors, as well as the importance of generating system-wide parameters of higher levels.

Key words: system-wide parameters; post-quantum electronic signature algorithms; algebraic lattices; hashing functions; cryptographic stability.

4 tab. 1 fig. Ref: 15 items.

УДК 004.056.55

Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / *Ю.І. Горбенко, М.В. Єсіна, В.В. Оноприєнко, Г.А. Малєєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 72 – 78.

Розглядається поняття моделі загроз, наводяться результати обґрунтування та розробка пропозицій щодо побудування моделі загроз стосовно асиметричних криптоперетворень типу перспективний електронний підпис (ЕП), що може застосовуватись в постквантовий період. Викладені узагальнені моделі загроз щодо перспективних ЕП та дається їх оцінка. Запропоновано моделі загроз щодо перспективних ЕП при застосуванні методів та засобів класичного та квантового криптоаналізу, моделі загроз при синтезі та застосуванні ЕП взагалі, а також моделі загроз при синтезі та застосуванні ЕП в постквантовий період. За результатами аналізу щодо методів синтезу та застосування відомих та перспективних ЕП визначено перелік загроз. Формулюються пропозиції щодо переліку загроз, щодо яких повинен бути забезпечений захист. Перелік загроз визначається за допомогою використання IT-Grundschutz Catalogues бази Германії, і на основі цього формується модель загроз. Визначається, що детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП повинні бути визначеними безумовно. Визначено основні загрози (методи) класичного криптоаналізу, що повинні бути враховані. Розглядаються можливі варіанти атак сторонніми каналами. Наведено основні загрози (атаки) із застосуванням квантових математичних методів, які можуть бути реалізовані на квантовому комп'ютері (звичайно, якщо він буде побудований). Наводиться порівняльний аналіз складності факторизації для класичного та квантового алгоритмів, а також порівняльний аналіз складності алгоритму дискретного логарифмування в скінченому полі на основі решета числового поля та алгоритму Шора. Розглядаються загрози (атаки) на прикладі проблеми стійкості криптоперетворень на основі навчання з помилками (LWE). У цілому атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі та атаки, що ґрунтуються на зведенні решіток. Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях.

Ключові слова: асиметричний ЕП; класичний та квантовий криптоаналіз; модель загроз при синтезі ЕП; модель загроз при застосуванні ЕП; перелік загроз ЕП; постквантовий період.

Табл. 3. Бібліогр.: 12 назв.

УДК 004.056.55

Модели угроз для асимметричных криптопреобразований перспективной электронной подписи / *Ю.И. Горбенко, М.В. Есина, В.В. Оноприенко, А.А. Малеева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 72 – 78.

Рассматривается понятие модели угроз, приводятся результаты обоснование и разработка предложений по построению модели угроз относительно асимметричных криптопреобразований типа перспективная электронная подпись (ЭП), что может применяться в постквантовый период. Изложены обобщенные модели угроз для перспективных ЭП и дается их оценка. Предложены модели угроз по перспективным ЭП при применении методов и средств классического и квантового криптоанализа, модели угроз при синтезе и применении ЭП вообще, а также модели угроз при синтезе и применении ЭП в постквантовый период. По результатам анализа по методам синтеза и применению известных и перспективных ЭП определен перечень угроз. Формулируются предложения относительно перечня угроз, в отношении которых должна быть обеспечена защита. Перечень угроз определялся с помощью использования IT-Grundschutz Catalogues базы Германии, и на основе этого формируется модель угроз. Определяется, что подробно угрозы по применению классического криптоанализа при синтезе и применении ЭП должны быть определены безусловно. Определены основные угрозы (методы) классического криптоанализа, которые должны быть учтены. Рассматриваются возможные варианты атак сторонними каналами. Приведены основные угрозы (атаки) с применением квантовых математических методов, которые могут быть реализованы на квантовом компьютере (конечно, если он будет построен). Приводится сравнительный анализ сложности факторизации для классического и квантового алгоритмов, а также сравнительный анализ сложности алгоритма дискретного логарифмирования в конечных полях на основе решета числового поля и алгоритма Шора. Рассматриваются угрозы (атаки) на примере проблемы устойчивости криптопреобразования на основе обучения с ошибками (LWE). В целом атаки на LWE можно разделить на два больших класса – атаки, основанные на переборе и атаки, основанные на приведении решеток. Предварительный анализ позволяет сделать вывод, что современные варианты механизмов LWE основываются на полиномиальных кольцах.

Ключевые слова: асимметричная ЭП; классический и квантовый криптоанализ; модель угроз при синтезе ЭП; модель угроз при применении ЭП; перечень угроз ЭП; постквантовый период.

Табл. 3. Библиогр.: 12 назв.

UDC 004.056.55

Threat models for asymmetric cryptotransformations of the promising electronic signature / *Yu.I. Gorbenko, M.V. Yesina, V.V. Onoprienko, G.A. Maleeva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 72 – 78.

The paper considers the concept of a threat model, presents the results of substantiation and development of proposals for building a threat model for asymmetric cryptotransformations such as a promising electronic signature (ES), which can be used in the post-quantum period. The generalized models of threats concerning perspective ES are stated in detail and their estimation is given. Threat models for promising ES using classical and quantum cryptanalysis methods and tools, threat models for synthesis and application of ES in general, as well as threat models for synthesis and application of ES in the post-quantum period are proposed. A list of threats is identified based on the results of the analysis of the methods of synthesis and application of known and promising ES. Proposals are formulated for a list of threats for which protection should be provided. The list of threats is determined using the IT-Grundschutz Catalogues of the German database, and based on this a threat model is formed. It is determined that the threats to the use of classical cryptanalysis in the synthesis and application of EP must be identified in detail unconditionally. The main threats (methods) of classical cryptanalysis that must be taken into account are identified. Possible variants of side channel attacks are considered. The main threats (attacks) using quantum mathematical methods that can be implemented on a quantum computer (of course, if it is built). A comparative analysis of the complexity of factorization for classical and quantum algorithms, as well as a comparative analysis of the complexity of the algorithm of discrete logarithm in a finite field based on the sieve of a numerical field and the Shore algorithm are given. Threats (attacks) are considered on the example of the problem of stability of cryptotransformations based on learning with errors (LWE). In general, attacks on LWE can be divided into 2 major classes – attacks based on bust and attacks based on lattice reduce. Preliminary analysis allows us to conclude that modern versions of LWE mechanisms are based on polynomial rings.

Key words: asymmetric ES; classical and quantum cryptanalysis; threat model in ES synthesis; threat model in ES application; list of ES threats; post-quantum period.

3 tab. Ref: 12 items.

УДК 004.056.55

Порівняльний аналіз ARX схем шифрування / *В.І. Руженцев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 79 – 86.

Аналізуються ARX алгоритми шифрування, тобто такі, що використовують лише три операції: модульне додавання, XOR додавання та циклічний зсув. Розробляються 16-бітні зменшені моделі найбільш відомих алгоритмів цього класу. Серед цих алгоритмів Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Деякі з них оперують 4-бітними словами, інші – 8-бітними словами. Шляхом вичерпного пошуку для моделей цих алгоритмів визначаються такі криптографічні показники, як максимальна імовірність проходження різниці (визначає стійкість шифру до атак диференціального криптоаналіза); максимальна імовірність лінійної апроксимації (визначає стійкість шифру до атак лінійного криптоаналіза); нелінійний порядок (визначає стійкість шифру до атак інтерполяційного, алгебраїчного криптоаналіза). Демонструється, що більшість моделей зі збільшенням кількості

циклів наближаються за цими показниками до параметрів випадкових підстановок. Визначено, що модель алгоритму Simon не володіє цією властивістю. Запропоновано декілька модифікацій цього алгоритму. Зіставляння кількості потрібних операцій для досягнення показників випадкової підстановки визначило найбільш вдалі ARX схеми. Найбільш ефективною 4-бітовою конструкцією є зменшена модель Chaskey, а найбільш ефективною 8-бітовою – запропонована в роботі модифікація схеми Simon. Показано, що, потенційно ARX схеми з більшим форматом операцій є більш гнучкими та ефективними, оскільки потребують приблизно вдвічі меншої кількості операцій для забезпечення криптографічних показників випадкової підстановки.

Ключові слова: криптоаналіз; стійкість; ARX-алгоритм; модульне додавання; циклічний зсув; диференційний криптоаналіз; різність; лінійний криптоаналіз; алгебраічний криптоаналіз; випадкова підстановка.

Табл. 5. Іл. 5. Бібліогр.: 20 назв.

УДК 004.056.55

Сравнительный анализ ARX схем шифрования / *В.И. Руженцев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 79 – 86.

Анализируются ARX алгоритмы шифрования, то есть такие, которые используют лишь три операции: модульное сложение, XOR сложение и циклический сдвиг. Разрабатываются 16-битные уменьшенные модели наиболее известных алгоритмов этого класса. Среди этих алгоритмов Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Некоторые из них оперируют 4-битными словами, другие – 8-битными словами. Путем исчерпывающего поиска для моделей этих алгоритмов определяются такие криптографические показатели, как максимальная вероятность прохождение разности (определяет стойкость шифра к атакам дифференциального криптоанализа); максимальная вероятность линейной аппроксимации (определяет стойкость шифра к атакам линейного криптоанализа); нелинейный порядок (определяет стойкость шифра к атакам интерполяционного, алгебраического криптоанализа). Демонстрируется, что большинство моделей с увеличением количества циклов приближаются по этим показателями к параметрам случайных подстановок. Определено, что модель алгоритма Simon не владеет этим свойством. Предложено несколько модификаций этого алгоритма. Сравнение количества нужных операций для достижения показателей случайной подстановки определило наиболее удачные ARX схемы. Наиболее эффективной 4-битовой конструкцией оказалась уменьшенная модель Chaskey, а наиболее эффективной 8-битовой – предложенная в работе модификация схемы Simon. Показано, что, потенциально, ARX схемы с большим форматом операций являются более гибкими и эффективными, поскольку требуют приблизительно вдвое меньшего количества операций для обеспечения криптографических показателей случайной подстановки.

Ключевые слова: криптоанализ; стойкость; ARX-алгоритм; модульное сложение; циклический сдвиг; дифференциальный криптоанализ; разность; линейный криптоанализ; алгебраический криптоанализ; случайная подстановка.

Табл. 5. Ил. 5. Библиогр.: 20 назв.

UDC 004.056.55

Comparative analysis of ARX encryption schemes / *V.I. Ruzhentsev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 79 – 86.

ARX encryption algorithms are analyzed, that is, those that use only three operations: modular addition, XOR addition and cyclic shift. 16-bit reduced models of the most famous algorithms of this class are being developed. Among these algorithms are Salsa, Chacha, Cypress, Speckey, Simon, Chaskey. Some of them operate with 4-bit words, others with 8-bit words. By an exhaustive search for models of these algorithms some cryptographic parameters are determined. These parameters are the maximum probability of passing the difference (determines the resistance of the cipher to attacks of differential cryptanalysis); maximum probability of linear approximation (determines the resistance of the cipher to attacks of linear cryptanalysis); non-linear order (determines the resistance of the cipher to interpolation attacks, algebraic cryptanalysis). It is demonstrated that most models with an increase in the number of rounds come to the parameters of random permutations. It is determined that the Simon algorithm model does not possess this property. Several modifications of this algorithm are proposed. Comparing the number of necessary operations to achieve random substitution performance, the most successful ARX schemes were determined. The most efficient 4-bit scheme is the reduced Chaskey model, and the most effective 8-bit one is the modification of the Simon scheme which was proposed in this work. It is shown that, potentially, ARX schemes with a large format of operations are more flexible and efficient, since they require approximately half the number of operations to provide cryptographic parameters of random substitution.

Key words: cryptanalysis; strength; ARX algorithm; modular addition; cyclic shift; differential cryptanalysis; difference; linear cryptanalysis; algebraic cryptanalysis; random substitution.

5 tab. 5 fig. Re

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОММУНІКАЦІЙНИХ СИСТЕМАХ
ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ
PROTECTION OF INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS

УДК 681.3.06:519.248.681

Методи та засоби синтезу і генерації сигналів – фізичних переносників даних у сучасних інформаційно-комунікаційних системах / *І.Д. Горбенко, Є.А. Семенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 87 – 98.

Функціонування низки сучасних інформаційно-комунікаційних систем (ІКС) здійснюється в умовах зовнішніх і внутрішніх впливів, обумовлених, з одного боку, дією природних перешкод, перешкод від інших радіотехнічних систем, що функціонують на близьких частотах або в спільній ділянці діапазону частот, з іншого боку, – навмисних завад, створюваних станціями протидії з метою радіоелектронного подавлення діючих систем. До ІКС, особливо, критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування: достовірності і швидкості передачі інформації, живучості, завадозахищеності, інформаційної безпеки. У таких умовах особливого значення набуває наявність і застосування захищених інформаційно-комунікаційних систем. Під захищеністю систем розуміють, перш за все, їх здатність забезпечувати необхідні показники з завадозахищеності, імітостійкості, інформаційної, енергетичної і структурної скритності, швидкості передавання інформації, частотної і енергетичної ефективності. Необхідність застосування захищених радіоканалів змушує дослідників по-новому подивитися на режими функціонування захищених радіоканалів і на аспекти формування і застосування складних сигналів – фізичних переносників даних для таких систем. У роботі представлено концептуальні положення щодо побудови захищених ІКС, які визначають необхідність проведення системної класифікації та уніфікацію інформаційних потоків для вирішення завдань формування та обробки інформації в ІКС, систематизацію моделей, методів, технічних і програмних засобів їх реалізації. Принципи побудови нових технологій в області ІКС повинні охоплювати весь спектр перетворень інформації в комплексі, від джерела до споживача, і повинні бути засновані не тільки на ефективній передачі інформації, але і на забезпеченні скритності, електромагнітної та іншої сумісності, екології, інформаційної безпеки, захищеності від нав'язування (введення в систему) помилкових даних і інше. Показано, що однією зі складних проблем створення захищених ІКС, є синтез системи сигналів – фізичних переносників даних. Наведено аналіз низки систем сигналів (OFDM-сигналів, сигналів з лінійною частотною модуляцією (ЛЧМ), складних нелінійних дискретних сигналів), застосування яких дозволяє поліпшити показники ефективності сучасних ІКС (завадостійкості прийому, інформаційної безпеки, скритності функціонування, захищеності від введення (нав'язування) неправдивих повідомлень, фальсифікації повідомлень; забезпечення цілісності даних, стійкості до міжсимвольної інтерференції, інформаційної ємності системи при обмеженій смузі пропускання, швидкості прийому-передачі даних тощо). У даній роботі на основі дослідження алгебраїчної структури систем нелінійних параметричних нерівностей сформульовані і у загальному виді вирішені задачі синтезу одного з нових класів складних нелінійних дискретних сигналів із заданими кореляційними, ансамблевими і структурними властивостями, – криптографічних сигналів. Представлено принципи побудови і загальна характеристика створеного програмно-апаратного комплексу для синтезу, дослідження властивостей, генерації, обробки та тестування математичних моделей низки класів сигналів-фізичних переносників даних у сучасних ІКС.

Ключові слова: завадостійкість прийому; скритність; інформаційна безпека; дискретні послідовності; складні системи сигналів; синтез систем сигналів; комплексний програмний засіб; інтерфейс користувача; шумоподібний сигнал.

Іл. 2. Бібліогр.: 16 назв.

УДК 681.3.06:519.248.681

Методы и средства синтеза и генерации сигналов – физических переносчиков данных в современных информационно-коммуникационных системах / *И.Д. Горбенко, Е.А. Семенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 87 – 98.

Функционирование ряда современных информационно-коммуникационных систем (ИКС) осуществляется в условиях внешних и внутренних воздействий, обусловленных, с одной стороны, действием естественных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот, с другой стороны, – помех, создаваемых станциями противодействия с целью радиоэлектронного подавления действующих систем. К ИКС, особенно критического назначения, предъявляются все более жесткие требования по обеспечению эффективности их функционирования: достоверности и скорости передачи информации, живучести, помехозащищенности, информационной безопасности. В таких условиях особое значение приобретает наличие и применение защищенных информационно-коммуникационных систем. Под защищенностью систем понимают, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности, скорости передачи информации, частотной и энергетической эффективности. Необходимость применения защищенных радиоканалов заставляет исследователей по-новому посмотреть на режимы функционирования защищенных радиоканалов и на аспекты формирования и применения сложных сигналов – физических переносчиков данных для таких систем. В работе представлены концептуальные положения по построению защищенных ИКС, которые определяют необходимость проведения системной классификации и унификации информацион-

ных потоков для решения задач формирования и обработки информации в ИКС, систематизацию моделей, методов, технических и программных средств их реализации. Принципы построения новых технологий в области ИКС должны охватывать весь спектр преобразований информации в комплексе – от источника к потребителю, должны быть основаны не только на эффективной передачи информации, но и на обеспечении скрытности, электромагнитной и другой совместимости, экологии, информационной безопасности, защищенности от навязывания (введение в систему) ошибочных данных и прочее. Показано, что одной из сложных проблем создания, защищенных ИКС является синтез системы сигналов – физических переносчиков данных. Проведен анализ ряда систем сигналов (OFDM-сигналов, сигналов с линейной частотной модуляцией (ЛЧМ), сложных нелинейных дискретных сигналов), применение которых позволяет улучшить показатели эффективности современных ИКС (помехоустойчивости приема, информационной безопасности, скрытности функционирования, защищенности от введения (навязывания) ложных сообщений фальсификации сообщений, обеспечения целостности данных, устойчивости к межсимвольной интерференции, информационной емкости системы при ограниченной полосе пропускания, скорости приема-передачи данных и т.д.). В работе на основе исследования алгебраической структуры систем нелинейных параметрических неравенств сформулирована и в общем виде решена задача синтеза одного из новых классов сложных нелинейных дискретных сигналов с заданными корреляционными, ансамблевыми и структурными свойствами, – криптографических сигналов. Представлены принципы построения и общая характеристика созданного программно-аппаратного комплекса для синтеза, исследования свойств, генерации, обработки и тестирования математических моделей ряда классов сигналов – физических переносчиков данных в современных ИКС.

Ключевые слова: помехоустойчивость приема; скрытность; информационная безопасность; дискретные последовательности; сложные системы сигналов; синтез систем сигналов; комплексное программное средство; интерфейс пользователя; шумоподобный сигнал.

Ил. 2. Библиогр.: 16 назв.

UDC 681.3.06:519.248.681

Methods and means of synthesis and generation of signals – physical carriers of data in modern information and communication systems / *I.D. Gorbenko, E.A. Semenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 87 – 98.

The functioning of a number of modern information and communication systems (ICS) is carried out under conditions of external and internal influences caused, on the one hand, by the action of natural interference, interference from other radio systems operating at close frequencies or in a common part of the frequency range, on the other hand , interference created by counteraction stations for the purpose of electronic suppression of existing systems. Increasingly stringent requirements are imposed on the ICS, especially for critical purposes, to ensure the efficiency of their functioning: the reliability and rate of information transfer, survivability, noise immunity, information security. In such conditions, the availability and use of secure information and communication systems is of particular importance. Under the security of systems is understood, first of all, their ability to provide the necessary indicators for noise immunity, imitation resistance, information, energy and structural secrecy, information transfer rate, frequency and energy efficiency. The need to use secure radio channels forces researchers to look in a new way, both at the modes of functioning of secure radio channels, and at the aspects of the formation and use of complex signals – physical data carriers for such systems. The paper presents conceptual provisions for the construction of secure ICS, which determine the need for a system classification and unification of information flows to solve the problems of information formation and processing in ICS, systematization of models, methods, hardware and software for their implementation. The principles of building new technologies in the field of ICS should cover the entire spectrum of information transformations in a complex, from a source to a consumer, and should be based not only on the effective transfer of information, but also on ensuring secrecy, electromagnetic and other compatibility, ecology, information security, protection from imposing (introduction into the system) of erroneous data and so on. It is shown that one of the complex problems of creating protected ICS is the synthesis of a system of signals – physical data carriers. The paper gives the analysis of a number of signal systems (OFDM – signals, signals with linear frequency modulation (LFM), complex nonlinear discrete signals), the use of which makes it possible to improve the efficiency indicators of modern ICS (reception noise immunity, information security, secrecy of functioning, protection from the introduction (imposition) of false messages, falsification of messages, ensuring data integrity, resistance to intersymbol interference, information capacity of the system with limited bandwidth, data transmission speed, etc.). In this paper, based on the study of the algebraic structure of systems of nonlinear parametric inequalities, the problem of synthesizing one of the new classes of complex nonlinear discrete signals with given correlation, ensemble and structural properties, cryptographic signals, is formulated and solved in a general form. The principles of construction and general characteristics of the created software and hardware complex for the synthesis, study of properties, generation, processing and testing of mathematical models of a number of classes of signals – physical data carriers in modern ICS.

Key words: reception immunity; secrecy; information security; discrete sequences; complex signal systems; synthesis of signal systems; complex software tool; user interface; noise-like signal.

2 fig. Ref: 16 items.

УДК 681.3.067+621.396.626:537.87

Врахування інтерференційної складової в технічному каналі витоку інформації побічного електромагнітного випромінювання відеотракту при рознесених прийомі / *В.Р. Воронов, В.І. Заболотний, В.І. Лиско* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 99 – 105.

Національними стандартами України, іншими нормативно-правовими документами системи технічного захисту інформації пропонується здійснювати захист відомостей, що становлять державну та іншу таємницю на об'єктах інформаційної діяльності організацій і установ всіх форм власності. Одним з небезпечних технічних каналів витоку інформації є канал побічних електромагнітних випромінювань відеотракту засобів електронно-обчислювальної техніки. Важливим елементом такого каналу є засоби радіо-, радіотехнічної розвідки, що використовуються зацікавленою стороною для перехоплення побічних електромагнітних випромінювань. Одним із напрямів удосконалення застосування засобів розвідки є рознесений прийом побічних електромагнітних випромінювань. При оцінці можливостей рознесеного прийому необхідно враховувати явища інтерференції відбитого від поверхні землі сигналу з сигналом прямого поширення від засобу електронно-обчислювальної техніки до прийомних антен розвідки.

Стаття присвячена аналізу необхідності врахування інтерференційного множника поширення електромагнітних полів при оцінці можливості ведення розвідки побічних електромагнітних випромінювань при рознесеному прийомі. Визначено підходи для врахування чинників впливу на інтерференцію ПЕМВ. Запропоновано складові частини кількісної моделі технічного каналу витоку інформації, що дозволяють проводити врахування факторів, що впливають на співвідношення сигнал/шум сигналу, що сприймається апаратурою розвідки.

Ключові слова: побічні електромагнітні випромінювання; інтерференція радіосигналів; рознесений прийом; сигнал / шум.

Іл. 4. Бібліогр.: 7 назв.

УДК 681.3.067+621.396.626:537.87

Учет интерференционной составляющей в техническом канале утечки информации побочного электромагнитного излучения видеотракта при разнесенном приеме / *В.Р. Воронов, В.И. Заболотный, В.И. Лыско* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 99 – 105.

Национальными стандартам Украины, другими нормативно-правовыми документами системы технической защиты информации предписывается осуществлять защиту сведений, составляющих государственную и другую тайну на объектах информационной деятельности организаций и учреждений всех форм собственности. Одним из опасных технических каналов утечки информации является канал побочных электромагнитных излучений видеотракта средств электронно-вычислительной техники. Важным элементом такого канала являются средства радио-, радиотехнической разведки, используемые заинтересованной стороной для перехвата побочных электромагнитных излучений. Одним из направлений совершенствования применения средств разведки является разнесенный прием побочных электромагнитных излучений. При оценке возможностей разнесенного приема необходимо учитывать также явления интерференции отраженного от поверхности земли сигнала с сигналом прямого распространения от средства электронно-вычислительной техники к приемным антеннам разведки.

Статья посвящена анализу необходимости учета интерференционного множителя распространения электромагнитных полей при оценке возможности ведения разведки побочных электромагнитных излучений при разнесенном приеме. Определены подходы для учета факторов влияния на интерференцию ПЭМВ. Предложены составные части количественной модели технического канала утечки информации, позволяющие проводить учет факторов, влияющих на соотношение сигнал/шум разведываемого сигнала в аппаратуре разведки.

Ключевые слова: побочные электромагнитные излучения; интерференция радиосигналов; разнесенный прием; сигнал/шум,

Ил. 4. Библиогр.: 7 назв.

UDC 681.3.067+621.396.626:537.87

Accounting for the interference component in the technical channel of information leakage of spurious electromagnetic radiation in the video path with diversity reception / *V.R. Voronov, V.I. Zabolotny, V.I. Lysko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 99 – 105.

National standards of Ukraine, other legal documents of the system of technical protection of information propose to protect information that is a state and other secret on the objects of information activities of organizations and institutions of all forms of ownership. One of the dangerous technical channels of information leakage is the channel of incidental electromagnetic radiation of the video path of electronic computing equipment. An important element of such a channel is the means of radio and radio intelligence used by the stakeholder to intercept spurious electromagnetic radiation. Intelligence tools are evolving and improving. One of the ways to improve the use of intelligence is the remote reception of incidental electromagnetic radiation. When assessing the possibilities of spaced reception, it is also necessary to take into account the phenomena of interference of the signal reflected from the earth's surface with the signal of direct propagation from the computer to the reconnaissance antennas.

The article is devoted to the analysis of the need to take into account the interference multiplier of electromagnetic field propagation when estimating the possibility of conducting reconnaissance of incidental electromagnetic radiation at spaced reception. Approaches to take into account the factors influencing the interference of PEMV are identified.

The components of the quantitative model of the technical channel of information leakage are proposed, which allow taking into account the factors influencing the signal/noise ratio of the signal perceived by the intelligence equipment.

Key words: spurious electromagnetic radiation; interference of radio signals; spaced reception; signal/noise.

4 fig. Ref: 7 items.

УДК 621.391

Комплексне вирішення проблеми електромагнітної сумісності сучасних інформаційно-комунікаційних систем / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 106 – 115.

Проаналізовано проблематику електромагнітної сумісності (ЕМС) інформаційно-комунікаційних систем (ІКС), розрахованих на багато користувачів, що використовують в якості способу надання доступу безлічі абонентів до ресурсів системи кодове розділення, при якому кожен абонент займає всю частотну смугу і весь часовий інтервал. Показано, що проблема електромагнітної сумісності ІКС як можливість безконфліктного існування різних бездротових ІКС в умовах, коли кожна з цих систем має можливість приймати свої сигнали і сигнали інших систем, є однією з найбільш пріоритетних при проєктуванні і експлуатації таких систем. Показана можливість реалізації вимог ЕМС на основі застосування широкосмугових шумоподібних сигналів (ШСС) в якості сигналів синхронізації і сигналів – фізичних переносників даних в умовах різних впливів, що заважають, в тому числі: вузькосмугових, широкосмугових загороджувальних, внутрішньосистемних (імітаційних, ретрансльованих) та інших завад, що створюються сусідніми станціями. Така можливість забезпечується завдяки застосуванню сигналів з великим значенням частотно-часового добутку (бази сигналу) без збільшення тривалості сигналу і пікової потужності випромінювання. На основі використання критерію розрізнення сигналів – мінімуму середньоквадратичної відстані між сигналами (векторами), сформульовані вимоги до синтезу і вибору класів ШСС, що забезпечують виконання вимог ЕМС бездротових систем зв'язку, розрахованих на багато користувачів. В якості сигналів-переносників даних і сигналів синхронізації запропоновано новий клас складних нелінійних дискретних криптографічних сигналів. Показано, що використання таких сигналів внаслідок того, що вони мають поліпшені ансамблеві, кореляційні, структурні властивості, дозволить здійснити комплексне вирішення проблеми ЕМС сучасних ІКС.

Ключові слова: електромагнітна сумісність; функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, оцінка параметрів сигналу; завадостійкість прийому сигналів; криптографічний сигнал; база сигналу; спектр частот.

Табл. 2. Бібліогр.: 10 назв.

УДК 621.391

Комплексное решение проблемы электромагнитной совместимости современных информационно-коммуникационных систем / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 106 – 115.

Проведен анализ проблематики электромагнитной совместимости (ЭМС) многопользовательских информационно-коммуникационных систем (ИКС), использующих в качестве способа предоставления доступа множества абонентов к ресурсам системы кодовое разделение, при котором каждый абонент занимает всю частотную полосу и весь временной интервал. Показано, что проблема электромагнитной совместимости ИКС как возможность бесконфликтного существования различных беспроводных ИКС в условиях, когда каждая из этих систем имеет возможность принимать свои сигналы и сигналы других систем, является одной из наиболее приоритетных при проектировании и эксплуатации таких систем. Показана возможность реализации требований ЭМС на основе применения широкополосных шумоподобных сигналов (ШШС) в качестве сигналов синхронизации и сигналов – физических переносчиков данных в условиях различных мешающих воздействий, в том числе: узкополосных, широкополосных заградительных, внутрисистемных (имитационных, ретранслированных) и других помех, создаваемыми соседствующими станциями. Такая возможность обеспечивается благодаря применению сигналов с большим значением частотно-временного произведения (базы сигнала) без увеличения длительности сигнала и пиковой мощности излучения. На основе использования критерия различимости сигналов – минимума среднеквадратического расстояния между сигналами (векторами) сформулированы требования к синтезу и выбору классов ШШС, обеспечивающих выполнение требований ЭМС многопользовательских беспроводных систем связи. Предложен, в качестве сигналов-переносчиков данных и сигналов синхронизации, новый класс сложных нелинейных дискретных криптографических сигналов. Показано, что использование таких сигналов вследствие того, что они обладают улучшенными ансамблевыми, корреляционными, структурными свойствами, позволит осуществить комплексное решение проблемы ЭМС современных ИКС.

Ключевые слова: электромагнитная совместимость; функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, оценка параметров сигнала; помехоустойчивость приема сигналов; криптографический сигнал; база сигнала; спектр частот.

Табл. 2. Библиогр.: 10 назв.

UDC 621.391

Comprehensive solution to the problem of electromagnetic compatibility of modern information and communication systems / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 106 – 115.

The analysis of the problems of electromagnetic compatibility (EMC) of multi-user information and communication systems (ICS), using code division as a way of providing multiple subscribers access to system resources, in which each subscriber occupies the entire frequency band and the entire time interval. It is shown that the problem of electromagnetic compatibility of ICS as the possibility of a conflict-free existence of various wireless ICS in the conditions when each of these systems has the ability to receive its signals and signals of other systems is one of the highest priorities in the design and operation of such systems. It is shown that EMC requirements can be realized through the use of broadband noise-like signals (BNLS) as synchronization signals and signals – physical data carriers under various interfering influences, including narrow-band, wide-band obstruction, intrasystem (imitated, relayed) and other interferences caused by neighboring stations. This possibility is provided due to the use of signals with a large value of the time-frequency product (signal base) without increasing the signal duration and peak radiation power. Based on the use of the criterion of distinguishability of the signals of the minimum root mean square distance between the signals (vectors), the requirements for the synthesis and selection of the BNLS classes are formulated to ensure that the EMC requirements of multi-user wireless communication systems are met. A new class of complex nonlinear discrete cryptographic signals is proposed as data carrier signals and synchronization signals. It is shown that the use of such signals, due to the fact that they have improved ensemble, correlation, and structural properties, will allow for a comprehensive solution to the EMC problem of modern ICS.

Key words: electromagnetic compatibility; correlation function; discrete sequences; synthesis of signal systems; noise-like signal, estimation of signal parameters; noise immunity of signal reception; cryptographic signal; signal base; frequency spectrum.

2 tab. Ref: 10 items.

УДК 681.3.06

Математична модель випадкової підстановки / *К.Є. Лисицький, І.В. Лисицька* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 116 – 124.

Обговорюються підходи до відбору випадкових підстановок, засновані на застосуванні системи критеріїв, побудованих з використанням оцінок близькості законів розподілу XOR таблиць і таблиць зміщень лінійних апроксимацій підстановок теоретичним законам, притаманним випадковим підстановкам. Відзначається їх неконструктивність. Неясно, які ж показники відбору є кращими.

Викладається сутність уточненої нами методики визначення законів розподілу максимумів для великих за обсягом вибірок незалежних однаково розподілених випадкових величин. Відзначається, що розподіл максимумів великих за обсягом вибірок незалежних однаково розподілених випадкових величин добре вивчено в теорії ймовірностей і описується розподілом екстремальних значень Фішера – Тіппета або log-Вейбула. Методика застосовується для визначення законів розподілів максимумів XOR таблиць і максимумів зсувів таблиць лінійних апроксимацій вибірки з байтових випадкових підстановок. Результати розрахунків порівнюються з результатами експериментів. Результати розрахунків і експериментів свідчать про те, що в обох випадках розподілу концентруються навколо досить виражених максимумів з цілком певними одними і тими ж найбільш ймовірними значеннями, що дозволяють вважати, що випадково згенеровані підстановки з великою ймовірністю будуть за значеннями максимумів мало відрізнятися один від одного.

На основі отриманих результатів пропонується уточнене визначення випадкової підстановки, яке будується на властивостях вибірки випадкових підстановок.

Відзначається, що застосування випадкових підстановок призводить до збільшення числа циклів приходу шифрів до стану випадкової підстановки на один цикл.

Робиться висновок, що випадкові підстановки, взяті з виходу генератора випадкових підстановок без всяких обмежень, цілком можуть конкурувати з кращими відомими конструкціями S-блоків, що використовуються в сучасних шифрах. Збільшені в порівнянні з граничними значення максимумів, до яких прагнуть автори більшості робіт з пошуку S-блоків з поліпшеними показниками, можуть бути компенсовані використанням в шифрі циклових функцій зі збільшеним числом S-блоків, що активізуються, на перших циклах.

Ключові слова: симетричний шифр; алгебраїчний імунітет; нелінійний вузол заміни; булева функція; закон розподілу максимумів; модель випадкової підстановки.

Табл. 4. Бібліогр.: 24 назв.

УДК 681.3.06

Математическая модель случайной подстановки / *К.Е. Лисицкий, И.В. Лисицкая* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 116 – 124.

Обсуждаются подходы к отбору случайных подстановок, основанные на применении системы критериев, построенных с использованием оценок близости законов распределения XOR таблиц и таблиц смещений линейных аппроксимаций подстановок теоретическим законам, присущим случайным подстановкам. Отмечается их неконструктивность. Неясно, какие же показатели отбора являются предпочтительными.

Излагается сущность уточненной нами методики определения законов распределения максимумов для больших по объему выборок независимых одинаково распределенных случайных величин. Отмечается, что распределение максимумов больших по объему выборок независимых одинаково распределенных случайных величин хорошо изучено в теории вероятностей и описывается распределением экстремальных значений Фишера – Типпета или log-Вейбула. Методика применяется для определения законов распределений максимумов XOR таблиц и максимумов смещений таблиц линейных аппроксимаций выборки из байтовых случайных подстановок. Результаты расчетов сравниваются с результатами экспериментов. Результаты расчетов и экспериментов свидетельствуют о том, что в обоих случаях распределения концентрируются вокруг достаточно выраженных максимумов с вполне определенными одними и теми же наиболее вероятными значениями, позволяющими считать, что случайно генерируемые подстановки с большой вероятностью будут по значениям максимумов мало отличаться друг от друга.

На основе полученных результатов предлагается уточненное определение случайной подстановки, которое строится на свойствах выборки случайных подстановок.

Отмечается, что применение случайных подстановок приводит к увеличению числа циклов прихода шифров к состоянию случайной подстановки на один цикл.

Делается вывод, что случайные подстановки, взятые с выхода генератора случайных подстановок без всяких ограничений, вполне могут конкурировать с лучшими известными конструкциями S-блоков, используемыми в современных шифрах. Увеличенные по сравнению с предельными значения максимумов, к которым стремятся авторы большинства работ по поиску S-блоков с улучшенными показателями, могут быть компенсированы использованием в шифрах цикловых функций с увеличенным числом активизируемых S-блоков на первых циклах.

Ключевые слова: симметричный шифр; алгебраический иммунитет; нелинейный узел замены; булева функция; закон распределения максимумов; модель случайной подстановки.

Табл. 4. Библиогр.: 24 назв.

UDC 681.3.06

Mathematical model of random substitution / *K. Lisitsky, I.V. Lysitskya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 116 – 124.

Approaches to the selection of random substitutions based on the application of a system of criteria constructed using estimates of the proximity of distribution laws of XOR tables and tables of displacements of linear approximations of substitutions to theoretical laws inherent in random substitutions are discussed. Their non-constructiveness is noted. It is not clear which selection rates are preferred.

The essence of our refined methodology for determining the laws of distribution of maxima for large samples of independent identically distributed random variables is stated. It is noted that the distribution of the maxima of large samples of independent identically distributed random variables is well studied in probability theory and is described by the distribution of Fisher-Tippett or log-Weibull extreme values. The technique is used to determine the laws of distribution of the maximums of XOR tables and the maximum of displacements of tables of linear approximations of a sample from byte random substitutions. The calculation results are compared with the experimental results. The results of calculations and experiments indicate that, in both cases, the distributions are concentrated around sufficiently pronounced maxima with quite definite and the same most probable values, which make it possible to assume that randomly generated substitutions with a high probability will differ little from each other in the values of the maxima.

Based on the results obtained, a refined definition of random substitution is proposed, which is based on the properties of a sample of random substitutions.

It is noted that the use of random substitutions leads to an increase in the number of cycles of arrival of ciphers to the state of random substitution by one cycle.

It is concluded that random substitutions taken from the output of a random substitution generator without any restrictions can compete with the best known S-box constructions used in modern ciphers. The maxima that are increased in comparison with the limiting values, which the authors of most works on the search for S-boxes with improved indicators strive for, can be compensated for by using cyclic functions in ciphers with an increased number of activated S-boxes in the first cycles.

Key words: symmetric cipher; algebraic immunity; non-linear replacement node; boolean function; distribution law of maxima; random substitution model.

4 tab. Ref: 24 items.

ОБРОБКА СИГНАЛІВ В РАДІОТЕХНІЧНИХ СИСТЕМАХ
ОБРАБОТКА СИГНАЛОВ В РАДИОТЕХНИЧЕСКИХ СИСТЕМАХ
SIGNAL PROCESSING IN RADIO ENGINEERING SYSTEMS

УДК 621.397

Обробка сигналів при пеленгації і визначенні дальності до малорозмірних БПЛА в оптичному і інфрачервоному діапазонах / *І.В. Корытцев, С.О. Шейко, В.М. Карташов, О.В. Зубков, В.М. Олейніков, С.І. Бабкін, І.С. Селезньов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 125 – 135.

Виявлення та оцінка координат БПЛА має вирішальне значення для захисту від їх несанкціонованого застосування в охоронюваних зонах. В роботі розглядається задача вибору алгоритму і параметрів обробки відеозображень стереопари в видимому, ближньому або дальньому інфрачервоному діапазонах для надійного визначення координат малих БПЛА, їх подальшого автосупроводу і оцінки параметрів руху. Проведено теоретичний аналіз можливостей оптичного методу двоканального стереовідеоспостереження. Представлено результати натурних експериментів з визначення координат малого БПЛА DJI Phantom 4 за допомогою системи стереовідеоспостереження на основі IP камер. Проведено калібрування зовнішніх і внутрішніх параметрів системи стереовідеоспостереження з урахуванням нелінійних спотворень об'єктивів. Калібрування камер здійснювалася в OpenCV за допомогою функції, заснованої на методах Zhang і Bouguet. Визначено теоретичні та практичні похибки вимірювання дальності до тестових об'єктів при їх різних положеннях. Описано алгоритм обробки зображень системи стереовідеоспостереження для виявлення, розпізнавання і вимірювання координат БПЛА. Наведено результати вимірювань координат БПЛА у двох тестових польотах. Вимірювання істинних координат БПЛА здійснювалося за даними бортового GPS приймача. Результати вимірювання азимута і кута місця БПЛА системою стереовідеоспостереження добре збігаються з даними GPS приймача. Це пояснюється високою роздільною здатністю камер і точним калібруванням їх внутрішніх параметрів. Середньоквадратична відносна похибка вимірювання дальності склала близько 10 %. Вказано шляхи для поліпшення точностних показників систем стереовідеоспостереження БПЛА.

Ключові слова: БПЛА; відеокамера; дальність; дрон; координати; виявлення; розпізнавання; ректифікація; стереобачення; трекінг.

Іл. 10. Бібліогр.: 24 назв.

УДК 621.397

Обработка сигналов при пеленгации и определении дальности до малоразмерных БПЛА в оптическом и инфракрасном диапазонах / *И.В. Корытцев, С.А. Шейко, В.М. Карташов, О.В. Зубков, В.Н. Олейников, С.И. Бабкин, И.С. Селезнев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 125 – 135.

Обнаружение и оценка координат БПЛА имеет решающее значение для защиты от их несанкционированного применения в охраняемых зонах. В работе рассматривается задача выбора алгоритма и параметров обработки видеоизображений стереопары в видимом, ближнем или дальнем инфракрасном диапазонах для надежного определения координат малых БПЛА, их последующего автосопровождения и оценки параметров движения. Проведен теоретический анализ возможностей оптического метода двуканального стереовидеонаблюдения. Представлены результаты натурных экспериментов по определению координат малого БПЛА DJI Phantom 4 с помощью системы стереовидеонаблюдения на основе IP камер. Проведена калибровка внешних и внутренних параметров системы стереовидеонаблюдения с учетом нелинейных искажений объективов. Калибровка камер осуществлялась в OpenCV при помощи функции, основанной на методах Zhang и Bouguet. Определены теоретические и практические погрешности измерения дальности до тестовых объектов при различных их положениях. Описан алгоритм обработки изображений системы стереовидеонаблюдения для обнаружения, распознавания и измерения координат БПЛА. Приведены результаты измерений координат БПЛА по двум тестовым полетам. Измерение истинных координат БПЛА осуществлялось по данным бортового GPS приемника. Результаты измерения азимута и угла места БПЛА системой стереовидеонаблюдения хорошо совпадают с данными GPS приемника. Это объясняется высокой разрешающей способностью камер и точной калибровкой их внутренних параметров. Среднеквадратическая относительная ошибка измерения дальности составила около 10 %. Указаны пути для улучшения точностных показателей систем стереовидеонаблюдения БПЛА.

Ключевые слова: БПЛА; видеокамера; дальность; дрон; координаты; обнаружение; распознавание; ректификация; стереовидение; трекинг.

Ил. 10. Библиогр.: 24 назв.

UDC 621.397

Signal processing for direction finding and range determining to small UAVs in the optical and infrared ranges / *I.V. Koryttsev, S.O. Sheiko, V.M. Kartashov, O.V. Zubkov, V.M. Oleynikov, S.I. Babkin, I.S. Selieznov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 125 – 135.

Detection and assessment of UAV coordinates is critical to protect against their unauthorized use in protected areas. The paper considers the problem of choosing the algorithm and parameters of stereo pair video processing in the visible, near-infrared and far-infrared ranges for reliable determination of small UAVs coordinates, further tracking of them and evaluation of UAVs motion parameters. Theoretical analysis of the optical method possibilities for two-channel stereo-video observation is carried out. The paper presents the results of field experiments aimed to determine the coordinates of a small UAV DJI Phantom 4 using a stereo-video observation system based on IP cameras. The external and internal parameters of the stereo-video observation system were calibrated taking into account the nonlinear distortions of the lenses. The cameras were calibrated in OpenCV using a function based on Zhang and Bouguet methods. The theoretical and practical errors in measuring the range to test objects at their different positions were determined. An algorithm for image processing of a stereo-video observation system for detection, recognition and measurement of UAV coordinates is described. The results of measurements of UAV coordinates for two test flights are presented. The measurement of the true coordinates of the UAV was carried out according to the data of the onboard GPS receiver. The results of measuring the azimuth and elevation of the UAV by the stereo-video observation system were matched with the data of the GPS receiver. This fact can be explained by high resolution of the cameras and the precise

calibration of their internal parameters. The root-mean-square relative error in measuring the range was about 10%. Ways for improving the accuracy of UAV stereo-video observation systems are shown.

Key words: UAV; video camera; range; drone; coordinates; detection; recognition; rectification; stereo vision; tracking.

10 fig. Ref: 24 items.

УДК 629.7.022

Дослідженнефективності детектування та розпізнавання зображень дронів за відеопотоком / *О.В. Зубков, С.О. Шейко, В.М. Олейніков, В.М. Карташов, І.В. Коритцев, С.І. Бабкін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 136 – 146.

Розроблено та експериментально протестовано алгоритм обробки відеопотоку стаціонарної відеокамери. Він складається з етапів виявлення рухомих об'єктів і класифікації цих об'єктів з використанням нейронної мережі. Для виявлення рухомих об'єктів використано методи виділення рухомих об'єктів на нерухомому фоні і аналізу історії руху. На підставі експериментальних даних проаналізовано ефективність застосування моделей заднього фону зображень MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP для вирішення поставленого завдання. Сформульовано рекомендації щодо вибору параметрів цих моделей. Критеріями вибору були: забезпечення високої швидкодії і низький рівень шумів. Для класифікації рухомих об'єктів створено і навченомоделі повнозв'язних і згортальних нейронних мереж, що дозволяють класифікувати 12 типів рухомих об'єктів. Для навчання нейронних мереж створено набори зображень: дронів, фрагментів листя дерев, трави, хмар і комах. На підставі результатів навчання та тестування мереж надано рекомендації до числа шарів мереж, числу нейронів в шарі, кількості згорток для досягнення максимальної швидкодії і точності розпізнавання. Порівняльний аналіз точності класифікації дронів із застосуванням повнозв'язних і згортальних мереж при обробці експериментальних даних довів ефективність застосування згортальних мереж. Побудовано залежність точності виявлення дрона від розміру зображення і, відповідно, від дальності до цього дрона.

Ключові слова: дослідження; ефективність; детектування; розпізнавання; зображення; дрон; відеопотік.

Табл. 3. Іл. 7. Бібліогр.: 20 назв.

УДК 629.7.022

Исследование эффективности детектированияи распознавания изображений дронов по видеопотоку / *О.В. Зубков, С.А. Шейко, В.Н. Олейников, В.М. Карташов, И.В. Корытцев, С.И. Бабкин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 136 – 146.

Разработан и экспериментально протестирован алгоритм обработки видеопотока стационарной видеокамеры. Он состоит из этапов обнаружения движущихся объектов и классификации этих объектов с использованием нейронной сети. Для обнаружения движущихся объектов использованы методы выделения движущихся объектов на неподвижном фоне и анализа истории движения. На основании экспериментальных данных проанализирована эффективность применения моделей заднего фона изображений MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP для решения поставленной задачи. Сформулированы рекомендации по выбору параметров этих моделей. Критерии выбора: обеспечение высокого быстродействия и низкий уровень шумов. Для классификации движущихся объектов созданы и обучены модели полносвязных и сверточных нейронных сетей, позволяющие классифицировать 12 типов подвижных объектов. Для обучения нейронных сетей созданы наборы изображений: дронов, фрагментов листвы деревьев, травы, облаков и насекомых. На основании результатов обучения и тестирования сетей даны рекомендации к числу слоев сетей, числу нейронов в слое, количеству сверток для достижения максимального быстродействия и точности распознавания. Сравнительный анализ точности классификации дронов с применением полносвязных и сверточных сетей при обработке экспериментальных данных доказал эффективность применения сверточных сетей. Построена зависимость точности обнаружения дрона от размера изображения и, соответственно, от дальности до этого дрона.

Ключевые слова: исследование; эффективность; детектирование; распознавание; изображение; дрон, видеопоток.

Табл. 3. Ил. 7. Библиогр.: 20 назв.

UDC 629.7.022

Study of the efficiency of detecting and recognizing drone images from a video stream / *O.V. Zubkov, S.A. Sheyko, V.N. Oleynikov, V.M. Kartashov, I.V. Korytsev, S.I. Babkin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 136 – 146.

The authors have developed and experimentally tested an algorithm for processing a video stream of a stationary video camera. It consists of the stages of detecting moving objects and classifying these objects using a neural network. To detect moving objects, the methods of identifying moving objects against a stationary background and analyzing the history of motion were used. Based on the experimental data, the effectiveness of using the models of the background images of MOG, MOG2, KNN, GMG, CNT, GSOC, LSBP for solving the problem was analyzed. Recommendations for the choice of the parameters of these models were formulated. The selection criteria were as follows: high performance and low noise. Models of fully connected and convolutional neural networks were created and trained making it possible to classify 12 types of moving objects. Sets of images were created to train neural networks: drones, fragments of tree foliage, grass, clouds and insects. Based on the results of training and testing networks, recommendations are

given for the number of network layers, the number of neurons in a layer, the number of convolutions to achieve maximum performance and recognition accuracy. Comparative analysis of the accuracy of drone classification using fully connected and convolutional networks when processing experimental data has proven the effectiveness of using convolutional networks. The dependence of the drone detection accuracy on the image size and, accordingly, on the distance to this drone is plotted.

Key words: research; efficiency; detection; recognition; image; drone; video stream.

3 tab. 7 fig. Ref: 20 items.

УДК 551.501.7

Аналіз частотно-часової структури акустичних шумів малих автоматичних аеросистем / *В.І. Леонідов, В.В. Семенець* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 147 – 152.

Формулюється постановка завдання виявлення малих автоматичних аеросистем (дронов), обґрунтовується доцільність побудови системи виявлення дронів на принципі прийому й аналізу акустичних сигналів, що випромінюються дронами під час виконання ними польотного завдання.

Дослідження часових флуктуацій періоду акустичних сигналів дрона проводиться методом модельно-кореляційного аналізу, у результаті якого формуються тривимірні структури: час – період – коефіцієнт кореляції акустичного сигналу з моделлю у вигляді обмеженої в часі синусоїдальної функції.

Отримані структури формуються у вигляді матриць значень коефіцієнта кореляції.

Члени, які розташовуються уздовж стовпців, розраховані при часовому зрушенні модельної функції уздовж вибірки сигналу. Члени в кожному стовпці розраховані при постійному, заданому з ряду значень, періоді модельної функції.

Показано, що коефіцієнти кореляції між рядками матриць, розрахованих по сигналах дрона значно більше, ніж ті ж значення, що отримані по вимірах фонового шуму. Функції, що показують зміну в часі коефіцієнтів кореляції між рядками матриць структур час – період для сигналів дрона й фонового шуму, не перетинаються й показують стійко більшу різницю коефіцієнтів кореляції, що дозволяє використати коефіцієнт кореляції як ознака що класифікує при розпізнаванні сигналів дрона.

Ключові слова: автоматичні аеросистеми; акустичний шум; кореляційний аналіз; модель сигналу; ознака.

Іл. 4. Бібліогр.: 12 назв.

УДК 551.501.7

Анализ частотно-временной структуры акустических шумов малых автоматических аэросистем / *В.И. Леонидов, В.В. Семенец* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 147 – 152.

Формулируется постановка задачи обнаружения малых автоматических аэросистем (дронов), обосновывается целесообразность построения системы обнаружения дронов на принципе приема и анализа акустических сигналов, излучаемых дронами во время выполнения ими полетного задания.

Исследование временных флуктуаций периода акустических сигналов дрона проводится методом модельно-корреляционного анализа, в результате которого формируются трехмерные структуры время – период – коэффициент корреляции акустического сигнала с моделью в виде ограниченной во времени синусоидальной функции.

Полученные структуры формируются в виде матриц значений коэффициента корреляции.

Члены, которые располагаются вдоль столбцов, рассчитаны при временном сдвиге модельной функции вдоль выборки сигнала. Члены в каждом столбце рассчитаны при постоянном, заданном из ряда значений, периоде модельной функции.

Показано, что коэффициенты корреляции между строками матриц, рассчитанных по сигналам дрона, значительно больше, чем те же значения, полученные по измерениям фонового шума. Функции, показывающие изменение во времени коэффициентов корреляции между строками матриц структур время – период для сигналов дрона и фонового шума, не пересекаются и показывают устойчиво большую разность коэффициентов корреляции, что позволяет использовать коэффициент корреляции в качестве классифицирующего признака при распознавании сигналов дрона.

Ключевые слова: автоматические аэросистемы; акустический шум; корреляционный анализ; модель сигнала; классифицирующий признак.

Ил. 4. Библиогр.: 12 назв.

UDC 551.501.7

Analysis of frequency-time structure of acoustic noise of small automatic air systems / *V.I. Leonidov, V.V. Semenets* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 147 – 152.

The statement of the problem of detecting small automatic air systems (drones) is formulated, the expediency of building a drone detection system on the principle of receiving and analyzing acoustic signals emitted by drones during their flight mission is substantiated.

The study of temporal fluctuations of the period of the acoustic signals of the drone is carried out by the method of model-correlation analysis, as a result of which three-dimensional structures are formed: time – period – the correlation coefficient of the acoustic signal with the model in the form of a sinusoidal function limited in time.

The resulting structures are formed as matrices of correlation coefficient values.

The members located along the columns are calculated with the time shift of the model function along the signal sample. The members in each column are calculated for a constant period of the model function set from a number of values.

It is shown that the correlation coefficients between the matrix rows calculated from the drone signals are significantly higher than the same values obtained from the background noise measurements. The functions showing the change in time of the correlation coefficients between the rows of the matrices of the time – period structures for drone signals and background noise do not intersect and show a consistently large difference in the correlation coefficients, which allows the correlation coefficient to be used as a classifying feature when recognizing drone signals.

Key words: automatic air systems; acoustic noise; correlation analysis; signal model; classifying feature.

4 fig. Ref: 12 items.

УДК 629.7.022

Оптико-електронні методи виявлення повітряних об’єктів та вимірювання їхніх координат / *В.М. Карташов, І.В. Коритцев, С. О. Шейко, В.М. Олейніков, О.В. Зубков, С.І. Бабкін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 153 – 159.

Проведено аналіз оптико-електронних методів (ОЕМ) з метою вибору і дослідження ОЕМ, здатного вирішувати завдання виявлення і визначення координат малих безпілотних літальних апаратів. Для даного застосування розглянуто різні ОЕМ вимірювання дальності до об'єктів. Оптико-електронні методи (ОЕМ) в режимах вимірювань характеризуються високою точністю, що обумовлює їх успішну інтеграцію з радіоелектронними комплексами різного призначення. Авторами запропоновано класифікувати ОЕМ за фізичним принципом на дві великі групи: активні і пасивні ОЕМ вимірювання дальності. Оцінено інтерференційні і модуляційні методи. Розглянуті активні методи мають високу точність, але вимагають значних енергетичних витрат і не забезпечують скритність роботи. Більш глибоко розглянуто пасивні ОЕМ вимірювання дальності. ОЕМ з матричними сенсорами поділяються на однокамерні і стереоскопічні. Особливий інтерес представляють методи, які не потребують участі зорового апарату людини в знятті вимірювальних відліків і забезпечують повну автоматизацію прийняття рішення. Розглянуті фоточутливі сенсори, що виявляють повітряні об'єкти, як вдень, так і вночі, мають матричну структуру і можуть бути інтегровані в єдину оптико-електронну систему виявлення і вимірювання дальності. Перевагою матричних ОЕМ є можливість одночасного використання всіх трьох датчиків денного, нічного та теплового бачення, що дозволить проводити надійне виявлення, розпізнавання та вимірювання координат малих повітряних об'єктів.

Ключові слова: оптика; електрон; метод; виявлення; повітря; об’єкт; вимірювання; координата.

Іл. 1. Бібліогр.: 32 назв.

УДК 629.7.022

Оптико-электронные методы обнаружения воздушных объектов и измерения их координат / *В.М. Карташов, И.В. Корытцев, С. А. Шейко, В.Н. Олейников, О.В. Зубков, С.И. Бабкин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 153 – 159.

Проведен анализ оптико-электронных методов (ОЭМ) с целью выбора и исследования ОЭМ, способного решать задачи обнаружения и определения координат малых беспилотных летательных аппаратов. Для данного применения рассмотрены различные ОЭМ измерения дальности до объектов. Оптико-электронные методы (ОЭМ) в режимах измерений характеризуются высокой точностью, что обусловливает их успешную интеграцию с радиоэлектронными комплексами разного назначения. Авторами предложено классифицировать ОЭМ по физическому принципу на две большие группы: активные и пассивные ОЭМ измерения дальности. Оценены интерференционные и модуляционные методы. Рассмотренные активные методы обладают высокой точностью, но требуют значительных энергетических затрат и не обеспечивают скрытность работы. Более глубоко рассмотрены пассивные ОЭМ измерения дальности. ОЭМ с матричными сенсорами подразделяются на однокамерные и стереоскопические. Особый интерес представляют методы, не требующие участия зрительного аппарата человека в снятии измерительных отсчетов и обеспечивающие полную автоматизацию принятия решения. Рассмотренные фоточувствительные сенсоры, выявляющие воздушные объекты, как днем, так и ночью, имеют матричную структуру и могут быть интегрированы в единую оптико-электронную систему обнаружения и измерения дальности. Достоинством матричных ОЭМ является возможность одновременного использования всех трех датчиков дневного, ночного и теплового видения, что позволит проводить надежное обнаружение, распознавание и измерение координат малых воздушных объектов.

Ключевые слова: оптика; электрон; метод; обнаружение; воздух; объект; измерение; координата.

Ил. 1. Библиогр.: 32 назв.

UDC 629.7.022

Optoelectronic methods for detecting air objects and measuring their coordinates / *V.M. Kartashov, I.V. Korytsev, S.A. Sheyko, V.N. Oleynikov, O.V. Zubkov, S.I. Babkin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 153 – 159.

The analysis of optical-electronic methods (OEM) is carried out in order to select and study an OEM capable of solving the problems of detecting and determining the coordinates of small unmanned aerial vehicles. With this aim in view, various OEM measurements of distance to objects are considered. Optoelectronic methods (OEM) in the meas-

urement modes are characterized by high accuracy, which leads to their successful integration with electronic complexes for various purposes. The authors proposed to classify the OEM according to the physical principle into two large groups: active and passive OEM for measuring range. Interference and modulation methods are evaluated. The considered active methods are highly accurate, but require significant energy consumption and do not provide secrecy of work. Passive OEM range measurements are considered in more depth. The OEM with matrix sensors are subdivided into single-chamber and stereoscopic. Methods, that do not require the participation of the human visual apparatus in taking measurement readings and provide complete automation of decision-making, are of particular interest. The considered photosensitive sensors that detect air objects, both day and night, have a matrix structure and can be integrated into a single optoelectronic system for detecting and measuring range. The advantage of the matrix OEM is the ability to use simultaneously all three sensors for day, night and thermal vision, which will allow reliable detection, recognition and measurement of coordinates of small air objects.

Key words: optics; electron; method; detection; air; object; measurement; coordinate.
1 fig. Ref: 32 items.

УДК 621391: 629.052.3: 551.510.535

Особливості застосування теореми відліків при обробці вузькосмугових радіосигналів з відомою центральною частотою спектра / *Є.В. Рогожкін, Ю.І. Под'ячий, Л.Я. Ємельянов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 160 – 163.

Представлено варіант дискретизації вузькосмугових радіосигналів з відомою центральною частотою спектра, який дозволяє значно зменшити обсяг обчислювальних операцій при обробці таких сигналів без істотних втрат інформації про їхні параметри. У даному випадку вузькосмужність визначається співвідношенням ширини спектру прийнятого радіолокаційного сигналу та робочої частоти підсилювача проміжної частоти, з виходу якого сигнал надходить до аналого-цифрового перетворювача (АЦП). Проведено дослідження запропонованого способу дискретизації, в якому частота слідування опитувальних імпульсів АЦП визначається частотою опорного сигналу задаючої системи когерентної РЛС і вибирається за величиною кратно нижче робочої частоти підсилювача проміжної частоти. Синхронізація опитувальних імпульсів АЦП організована так, що будь-які два сусідніх відліки є квадратурно пов'язаними. Така процедура дозволяє визначити амплітуду і фазу сигналу, що відповідають кожному відліку. Тим самим створюються умови для визначення доплерівського зсуву і параметрів огинаючої сигналу. Наведено результати розрахунку відносної похибки визначення амплітуди сигналу, яка утворюється в результаті незбігу частоти прийнятого сигналу з частотою опорного сигналу. Для реальних випадків вона не перевищує 1 % і залежить від характеристик РЛС (довжина зондуючої хвилі, кратність між значенням проміжної частоти, на якій ведеться обробка, і значенням частоти відліків), а також від величини радіальної швидкості об'єкта і початкової різниці фаз між сигналом на виході підсилювача проміжної частоти й опорним сигналом. Показано, що такий підхід до перетворення сигналу в цифровий формат може бути застосований і для сигналів з фазовою $(0, \pi)$ маніпуляцією, якщо тривалість елементів коду суттєво більше періоду опорної частоти.

Ключові слова: обробка радіолокаційних сигналів; синхронне детектування; аналого-цифрове перетворення; дискретизація сигналу; доплерівський зсув.
Табл. 1. Іл. 2. Бібліогр.: 8 назв.

УДК 621391: 629.052.3: 551.510.535

Особенности применения теоремы отсчетов при обработке узкополосных радиосигналов с известной центральной частотой спектра / *Е.В. Рогожкин, Ю.И. Подъячий, Л.Я. Емельянов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 160 – 163.

Представлен вариант дискретизации узкополосных радиосигналов с известной центральной частотой спектра, который позволяет значительно уменьшить объем вычислительных операций при обработке таких сигналов без существенных потерь информации об их параметрах. В рассматриваемом случае узкополосность определяется соотношением ширины спектра принимаемого радиолокационного сигнала и рабочей частоты усилителя промежуточной частоты, с выхода которого сигнал поступает на аналого-цифровой преобразователь (АЦП). Исследован предложенный способ дискретизации, в котором частота следования опросных импульсов АЦП определяется частотой опорного сигнала задающей системы когерентной РЛС и выбирается по величине кратно ниже рабочей частоты усилителя промежуточной частоты. Синхронизация опросных импульсов АЦП организована так, что любые два соседних отсчета квадратурно связаны. Такая процедура позволяет определить амплитуду и фазу принимаемого сигнала, соответствующие каждому отсчету. Тем самым создаются условия для определения доплеровского сдвига и параметров огибающей сигнала. Приведены результаты расчета относительной погрешности определения амплитуды сигнала, которая образуется в результате несовпадения частоты принятого сигнала с частотой опорного сигнала. Для реальных случаев она не превышает 1 % и зависит от характеристик РЛС (длина зондирующей волны, кратность между значением промежуточной частоты, на которой ведется обработка, и значеним частоты отсчетов), а также от величины радиальной скорости объекта и начальной разности фаз между сигналом на выходе усилителя промежуточной частоты и опорным сигналом. Показано, что такой подход к преобразованию сигнала в цифровой формат применим и для сигналов с фазовой $(0, \pi)$ манипуляцией, если длительность элементов кода существенно больше периода опорного сигнала.

Ключевые слова: обработка радиолокационных сигналов; синхронное детектирование; аналого-цифровое преобразование; дискретизация сигнала; доплеровский сдвиг.

Табл. 1. Ил. 2. Библиогр.: 8 назв.

UDC 621391: 629.052.3: 551.510.535

Features of application of the sampling theorem when processing narrow-band radio signals with known center frequency of the spectrum / *E.V. Rogozhkin, Yu.I. Podyachiy, L.Ya. Emelyanov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 160 – 163.

An option is presented for sampling narrow-band radio signals with a known center frequency of the spectrum, which can significantly reduce the amount of computational operations when processing such signals without significant loss of information about their parameters. In this case, narrowband is determined by the ratio of the spectrum width of the received radar signal and the operating frequency of the intermediate frequency amplifier, from the output of which the signal is fed to an analog-to-digital converter (ADC). A study of the proposed method of discretization is carried out, in which the repetition rate of the ADC interrogation pulses is determined by the frequency of the reference signal of the master system of a coherent radar and is selected multiple times lower than the operating frequency of the intermediate frequency amplifier. The synchronization of the ADC interrogation pulses is organized in such a way that any two adjacent samples are quadrature connected. This procedure allows you to determine the amplitude and phase of the received signal corresponding to each sample. This creates the conditions for determining the Doppler shift and envelope parameters of the signal. The results of calculating the relative error in determining the amplitude of the signal, which appears as a result of a mismatch in the frequency of the received signal with the frequency of the reference signal, are presented. For real cases, it does not exceed 1% and depends on the radar characteristics (sounding wavelength, multiplicity between the value of the intermediate frequency at which the processing is carried out, and the value of the sampling frequency), as well as on the magnitude of the object radial velocity and the initial phase difference between the output signal of the intermediate frequency amplifier and the reference signal. It is shown that this approach to converting the signal into a digital format is also applicable to signals with phase (0, π) manipulation if the duration of the code elements is significantly longer than the period of the reference signal.

Key words: processing of radar signals; synchronous detection; analog-to-digital conversion; signal sampling; Doppler shift.

1 tab. 2 fig. Ref: 8 items.

УДК 004.89: 621.396

Предикатна модель процесних знань при виявленні і розпізнаванні протяжних об'єктів типу хмари, «ангел-луна» в оглядових РЛС / *С.В. Солонська, В.В. Жирнов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 164 – 172.

Розроблено предикатну модель процесних знань міжперіодної обробки радіолокаційних сигналів при виявленні і розпізнаванні протяжних об'єктів і метод прийняття рішень, заснований на прецедентах. Наведено основні особливості і структурні елементи моделі процесних знань. Показано, що переваги даної моделі пов'язані з можливостями конфігурації і ієрархічного представлення процесу з вивчення можливих структур одиночних або груп імпульсних сигналів в межах однієї зони огляду РЛС на основі інтелектуального аналізу сигналів з використанням алгебри кінцевих предикатів. Показано, як цей підхід може використовуватися для автоматизації процесу виявлення і розпізнавання протяжних об'єктів типу хмари, атмосферні неоднорідності типу «ангел-луна». Розроблено метод обробки процесних знань як інструмент для створення універсальних алгоритмів міжперіодной обробки сигнальної інформації для забезпечення ефективного виявлення і розпізнавання різних протяжних об'єктів, в тому числі атмосферних неоднорідностей типу «ангел-луна», за рахунок накопичення як сигнальної (енергетичної), так і логічної інформації в комірці, що аналізується, та в її околу. В розроблену технологію входять процедури формалізації та аналізу символьної моделі спостережуваних об'єктів для прийняття рішень, заснованих на прецедентах. Залежно від типів зв'язків, які використовуються в моделі, розрізняють класифіковані і функціональні мережі, де використовуються деякі елементи логічних і мережевих моделей. З логічних моделей запозичена ідея правил виведення або вирішального правила, а з мережевих моделей – опис знань у вигляді семантичної нейронної мережі. У цієї комбінованої моделі явно виділена процедурна інформація. Замість логічного висновку з'являється висновок або вирішальне правило на знаннях. В результаті рішення системи предикатних рівнянь процесних знань знаходимо місце, геометричні розміри і вид символьної моделі протяжного об'єкта.

Ключові слова: модель процесних знань; прийняття рішень; рухомий об’єкт; виявлення; розпізнавання; інтелектуальна система; символьна модель сигнальних відміток.

Іл. 4. Бібліогр.: 13 назв.

УДК 004.89: 621.396

Предикатная модель процессных знаний при обнаружении и распознавании протяженных объектов типа облака, тучи, «ангел-эхо» в обзорных РЛС / *С.В. Солонская, В.В. Жирнов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 164 – 172.

Разработана предикатная модель процессных знаний межпериодной обработки радиолокационных сигналов при обнаружении и распознавании протяженных объектов и метод принятия решений, основанный на

прецедентах. Приведены основные особенности и структурные элементы модели процессных знаний. Показано, что преимущества данной модели связаны с возможностями конфигурирования и иерархического представления процесса по изучению возможных структур одиночных или групп импульсных сигналов в пределах одной зоны обзора РЛС на основе интеллектуального анализа сигналов с использованием алгебры конечных предикатов. Показано, как этот подход может использоваться для автоматизации процесса обнаружения и распознавания протяженных объектов типа облака, тучи, атмосферные неоднородности типа «ангел-эхо». Разработан метод обработки процессных знаний как инструмент для создания универсальных алгоритмов межпериодной обработки сигнальной информации для обеспечения эффективного обнаружения и распознавания разных протяженных объектов, в том числе атмосферных неоднородностей типа «ангел-эхо», за счет накопления как сигнальной (энергетической), так и логической информации в анализируемой ячейке и в ее окрестности. В разработанную технологию входят процедуры формализации и анализа символьной модели наблюдаемых объектов для принятия решений, основанных на прецедентах. В зависимости от типов связей, используемых в модели, различают классифицирующие и функциональные сети, где используются некоторые элементы логических и сетевых моделей. Из логических моделей заимствована идея правил вывода или решающего правила, а из сетевых моделей – описание знаний в виде семантической нейронной сети. В этой комбинированной модели явно выделена процедурная информация. Вместо логического вывода появляется вывод или решающее правило на знаниях. В результате решения системы предикатных уравнений процессных знаний находим место, геометрические размеры и вид символьной модели протяженного объекта.

Ключевые слова: модель процессных знаний; принятия решений; протяженный объект; обнаружение; распознавание; интеллектуальная система; символьная модель.

Ил. 4. Библиогр.: 13 назв.

UDC 004.89: 621.396

Predicate model of process knowledge when detecting and recognizing extended objects such as clouds, angel-echoes in surveillance radars / *S. Solonskaya, V. Zhyrnov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 164 – 172.

A predicate model of the process knowledge of inter-period processing of radar signals in the detection and recognition of extended objects and a decision-making method based on precedents have been developed. The main features and structural elements of the process knowledge model are presented. It is shown that the advantages of this model are related to the configuration and hierarchical representation of the process for studying the possible structures of single or groups of impulse signals within the same radar field of view based on the intelligent analysis of signals using the algebra of finite predicates. It is shown how this approach can be used to automate the process of detecting and recognizing extended objects such as clouds, atmospheric inhomogeneities of the angel-echo type. A method for processing process knowledge has been developed as a tool for creating universal algorithms for inter-period processing of signal information to ensure effective detection and recognition of various extended objects, including atmospheric inhomogeneities of the angel-echo type, by accumulating both signal (energy) and logical information in the analyzed cell and in its vicinity. The developed technology includes procedures for formalizing and analyzing the symbolic model of observed objects for making decisions based on precedents. Depending on the types of connections used in the model, classifying and functional networks are distinguished, where some elements of logical and network models are used. The idea of inference rules or decision rules is borrowed from logical models, and the description of knowledge in the form of a semantic neural network is borrowed from network models. In this combined model, procedural information is clearly highlighted. Instead of a logical conclusion, a conclusion or a decisive rule on knowledge appears. As a result of solving the system of predicate equations of process knowledge, we find the place, geometric dimensions and type of the symbolic model of an extended object.

Key words: model of process knowledge; decision making; moving object; detection; recognition; intelligent system.

4 fig. Ref: 13 items.

УДК 621.397.48:004.932.2

Методи комплексної обробки та інтерпретації радіолокаційних, акустичних, оптичних і інфрачервоних сигналів безпілотних літальних апаратів / *В.М. Карташов, В.Н. Олейніков, В.П. Рябуха, С.И. Бабкін, В.В. Воронін, А.И. Капуста, И.С. Селєзнев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 173 – 182.

Безпілотні літальні апарати (БПЛА) знаходять широке застосування при вирішенні широкого спектра корисних завдань, а з іншого боку, вони здатні нести активну або пасивну потенційну загрозу для різних областей діяльності людини – господарській, повсякденній і військовій. З метою виявлення та вимірювання координат безпілотних літальних апаратів використовують радіолокаційні, акустичні, інфрачервоні і оптичні засоби.

Оскільки області можливостей різних методів не збігаються, то з'являється передумова спільного використання систем різного виду для розширення набору вимірюваних параметрів, діапазону спостережуваних діяльностей і підвищення інформативності одержуваних даних шляхом сумісній (комплексній) їх обробки. Комплексна обробка сигналів різних інформаційних каналів може здійснюватися як на етапі виявлення, так і на етапі

вимірювання координат. Причому на етапі виявлення вона найбільш затребувана в силу складності завдання виявлення-розпізнавання.

Число публікацій в даній області постійно збільшується, приділяється увага і комплексним системам, побудованим з використанням різних фізичних сенсорів. Однак ефективність функціонування систем з комплексною обробкою сигналів на практиці є недостатньою.

Стаття присвячена аналізу можливостей комплексних систем з обробкою многомодальної інформації, одержуваної по кожному з використовуваних каналів, а також розробці нових більш ефективних методів комплексування радіолокаційних, оптичних, інфрачервоних і акустичних каналів комплексних систем виявлення і вимірювання координат БПЛА.

Ключові слова: безпілотний літальний апарат; виявлення; розпізнавання; радіолокаційна станція; содар; відеокамера; комплексна система; обробка сигналів.

Іл. 5. Бібліогр.: 37 назв.

УДК 621.397.48:004.932.2

Методы комплексной обработки и интерпретации радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов / *В.М. Карташов, В.Н. Олейников, В.П. Рябуха, С.И. Бабкин, В.В. Воронин, А.И. Капуста, И.С. Селезнев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 173 – 182.

Беспилотные летательные аппараты (БПЛА) находят широкое применение при решении широкого спектра полезных задач, а с другой стороны, они способны нести активную или пассивную потенциальную угрозу для различных областей деятельности человека – хозяйственной, повседневной и военной. С целью обнаружения и измерения координат беспилотных летательных аппаратов в настоящее время используют радиолокационные, акустические, инфракрасные и оптические средства.

Поскольку области возможностей различных методов не совпадают, то появляется предпосылка совместного использования систем различного вида для расширения набора измеряемых параметров, диапазона наблюдаемых дальностей и повышения информативности получаемых данных путем совместной (комплексной) их обработки. Комплексная обработка сигналов различных информационных каналов может осуществляться как на этапе обнаружения, так и на этапе измерения координат. Причем на этапе обнаружения она наиболее востребована в силу сложности задачи обнаружения-распознавания.

Число публикаций в данной области постоянно увеличивается, уделяется внимание и комплексным системам, построенным с использованием различных физических сенсоров. Однако эффективность функционирования систем с комплексной обработкой сигналов на практике является недостаточной.

Статья посвящена анализу возможностей комплексных систем с обработкой многомодальной информации, получаемой по каждому из используемых каналов, а также разработке новых более эффективных методов комплексирования радиолокационных, оптических, инфракрасных и акустических каналов комплексных систем обнаружения и измерения координат БПЛА.

Ключевые слова: беспилотный летательный аппарат; обнаружение; распознавание; радиолокационная станция; содар; видеокамера; комплексная система; обработка сигналов.

Ил. 5. Библиогр.: 37 назв.

UDC 621.397.48:004.932.2

Methods for complex processing and interpretation of radar, acoustic, optical and infrared signals from unmanned aerial vehicles / *V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, S.I. Babkin, V.V. Voronin, A.I. Kapusta, I.S. Selezniov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 173 – 182.

Unmanned aerial vehicles (UAVs) are currently widely used in solving a wide range of useful tasks, and on the other hand, they are capable of carrying an active or passive potential threat to various areas of human activity, namely, economic, daily and military. Radar, acoustic, infrared and optical means are currently used to detect and measure the coordinates of unmanned aerial vehicles.

Since the areas of capabilities of different methods do not coincide, the prerequisite for the joint use of systems of various types appears to expand the set of measured parameters, the range of observed distances and increase the information content of the obtained data by joint (complex) processing. Complex processing of signals of various information channels can be carried out both at the stage of detection and at the stage of measuring coordinates. Moreover, at the detection stage, it is most in demand due to the complexity of the detection-recognition task.

The number of publications in this area is constantly increasing; attention is also paid to complex systems built using various physical sensors. However, the efficiency of functioning of the systems with complex signal processing in practice is not sufficient.

The article is devoted to the analysis of the capabilities of integrated systems with the processing of multimodal information obtained from each of the channels used, as well as the development of new more efficient methods for integrating radar, optical, infrared and acoustic channels of integrated systems for the detection and measurement of UAV coordinates.

Key words: unmanned aerial vehicle; detection; recognition; radar station; sodar; video camera; integrated system; signal processing.

5 fig. Ref: 37 items.

ПРИСТРОЇ РАДІОТЕХНІКИ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ
УСТРОЙСТВА РАДИОТЕХНИКИ И СРЕДСТВА ТЕЛЕКОММУНИКАЦИЙ
RADIO ENGINEERING DEVICES AND MEANS OF TELECOMMUNICATIONS

УДК 621.375.4

Фазові характеристики підсилювача класу Е з різними вихідними ланками / *В.Г. Крижановський* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 183 – 188.

Моделюванням та експериментально досліджено залежності зсуву фази від частоти у підсилювачах класу Е з класичною вихідною ланкою та вихідною ланкою з двократним виконанням умов класу Е на навантажувальний імпеданс. Аналітично розглянуто залежність зсуву фази на ключі в номінальному режимі. Досліджено зсув фаз на ключі у субоптимальному режимі роботи підсилювача класу Е, що виникає при зміні робочої частоти. Моделювання проведено методом гармонічного балансу на основі моделі ключа з урахуванням структури потужного польового транзистора – наявність вбудованого антипаралельного діоду, який змінює форму імпульсу напруги на ключі. Враховувались вхідна та перехідна ємності транзистора. Експериментальне вимірювання зсуву фаз проводилось на основі записаних оцифрованих форм напруги на вході та на виході ключа шляхом обчислення фаз перших гармонік напруги за допомогою швидкого перетворення Фурье. Встановлено залежність характеру зміни фази на виході ключа та підсилювача в цілому від виду навантажувальної ланки. Показаний зв'язок зсуву фази на ключі в залежності від годографу навантажувального імпедансу. Для ланки з двократним виконанням умов класу Е, що має петлю на годографі навантажувального імпедансу, залежність зсуву фази на ключі має екстремум, що потенційно надає можливість отримати однаковий зсув фаз на двох частотах робочого діапазону. Це дозволяє управляти фазочастотною характеристикою та груповим часом затримки підсилювача. Знання залежності зсуву фази від частоти дозволяє спростити умови визначення зсуву фази у колі зворотного зв'язку. Отримані результати будуть корисні для проєктування автогенераторів класу Е зі зміною частоти у широкому діапазоні.

Ключові слова: фазочастотна характеристика; підсилювач класу Е; автогенератор класу Е; МОН транзистор; умови класу Е.

Табл. 1. Іл. 12. Бібліогр.: 18 назв.

УДК 621.375.4

Фазовые характеристики усилителя класса Е с различными выходными цепями / *В.Г. Крыжановский* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 183 – 188.

Моделированием и экспериментально исследованы зависимости сдвига фазы от частоты в усилителях класса Е с классической выходной цепью и цепью с двукратным выполнением условий класса Е на погрузочный импеданс. Аналитически рассмотрена зависимость сдвига фазы на ключе в номинальном режиме. Исследован сдвиг фаз на ключе в субоптимальном режиме работы усилителя класса Е, возникающим при изменении рабочей частоты. Моделирование проведено методом гармонического баланса на основе модели ключа с учетом структуры мощного полевого транзистора – наличия встроенного антипараллельного диода, который изменяет форму импульса напряжения на ключе. Учитывались входная и переходная емкости транзистора. Экспериментальное измерение сдвига фаз проводилось на основе записанных оцифрованных форм напряжения на входе и на выходе ключа путем вычисления фаз первых гармоник напряжения с помощью быстрого преобразования Фурье. Установлена зависимость изменения фазы на выходе ключа и усилителя в целом от вида нагрузочной цепи. Показана связь сдвига фазы на ключе с формой годографа нагрузочного импеданса. Для звена с двукратным выполнением условий класса Е, с петлей на годографе нагрузочного импеданса, зависимость сдвига фазы на ключе от частоты имеет экстремум, что позволяет получить одинаковый сдвиг фаз на двух частотах рабочего диапазона. Это позволяет управлять фазочастотной характеристикой и групповым временем запаздывания усилителя. Знание зависимости сдвига фазы от частоты позволяет упростить условия определения сдвига фазы в цепи обратной связи. Полученные результаты могут быть полезными при проектировании автогенераторов класса Е с перестройкой частоты в широком диапазоне.

Ключевые слова: фазочастотная характеристика; усилитель класса Е; автогенератор класса Е; МОП транзистор; условия класса Е.

Табл. 1. Ил. 12. Библиогр.: 18 назв.

UDC 621.375.4

Phase characteristics of E class amplifier with various output networks / *V.G. Krizhanovski* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №202. P. 183 – 188.

Phase shift of E class amplifiers with classical output network and output network that satisfies E class loading impedance conditions twice in the frequency band were studied by simulation and experimentally. The phase shift across switch in nominal operation mode was investigated analytically. The phase shift across switch in suboptimal class E operation mode that occurs while altering the operation frequency was investigated as well. The simulation method was the harmonic balance analysis using the switch model that considers the structure of power MOSFET device, namely, the existence of antiparallel diode pair that alters the switch current waveform. The input and transition capacitances of the transistor were considered. Experimental measurement of the phase shift was performed utilizing the recorded digitized waveforms of the switch input and output voltages by computing the phases of the voltages' first harmonics with the help of Fast Fourier Transform. It was observed that characteristics of phase shift at switch output

and amplifier output are dependent on the kind of load network. The relationship between the phase shift at the switch and hodograph of the loading impedance was demonstrated. For the network with double fulfilment of class E conditions that has a loop in the loading impedance hodograph the switch phase shift dependency has an extremum, which provides an opportunity to obtain the same phase shift at two frequencies within the operating frequency band. That facilitates control of the phase-frequency characteristic and the group delay of the amplifier. Knowledge of the phase-frequency dependency simplifies the conditions for calculation of the phase shift in the feedback network. The obtained results are useful for design of class E oscillator operating in a wide frequency band.

Key words: phase frequency response; E class amplifier; E class oscillator; MOSFET; E class condition.

1 tab. 12 fig. Ref: 18 items.

ФІЗИКА ПРИСТРОЇВ ТА СИСТЕМ
ФИЗИКА ПРИБОРОВ И СИСТЕМ
PHYSICS OF DEVICES AND SYSTEMS

УДК 53.082.52

Дослідження інерційних характеристик фоторезисторів у фізичному практикумі / *О.М. Андреєв, О.М. Андреєва* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 189 – 195.

Описано вимірювальний комплекс на базі 32-розрядного мікроконтролера STM32F103VET6 для дослідження люкс-амперної (світлової), частотної та інерційної характеристик фоторезистора при різних законах рекомбінації нерівноважних носіїв заряду, що виникають під дією світла. Розроблена установка підключається до персонального комп'ютера (смартфона) та дозволяє аналізувати фронти наростання і спаду струму фоторезистора, а також визначати час життя надлишкових носіїв заряду при різних рівнях освітленості. На відміну від традиційних методів вимірювання параметрів фоторезисторів, що працюють в динамічному режимі, в запропонованій установці не використовуються осцилограф і окремий модулятор світлового потоку (генератор або переривник), це дозволило істотно зменшити габаритні розміри та собівартість комплексу, а також автоматизувати процес вимірювання. Для визначення частотної характеристики фоторезистора запропоновано використовувати синтезатор частоти, який дозволяє разом з цифро-аналоговим перетворювачем мікроконтролера сформувати амплітудно-модульований світловий потік необхідної частоти і глибини модуляції. Описаний комплекс може бути підключений до мережі інтернет за допомогою Wi-Fi модуля на базі мікроконтролера ESP8266, що дозволяє проводити дослідження в дистанційному режимі. Також передбачена можливість визначати параметри фоторезистора при різних значеннях опору навантаження.

Ключові слова: фоторезистор; фотопровідність; внутрішній фотоефект; фоторезистивний ефект; нерівноважні носії; час життя; люкс-амперна характеристика; мікроконтролер; синтезатор частоти.

Іл. 8. Бібліогр.: 10 назв.

УДК 53.082.52

Исследование инерционных характеристик фоторезисторов в физическом практикуме / *А.Н. Андреев, О.Н. Андреева* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 202. С. 189 – 195.

Описан измерительный комплекс на базе 32-разрядного микроконтроллера STM32F103VET6 для исследования люкс-амперной (световой), частотной и инерционной характеристик фоторезистора при разных законах рекомбинации неравновесных носителей заряда, возникающих под действием света. Разработанная установка подключается к персональному компьютеру (смартфону) и позволяет анализировать фронты нарастания и спада тока фоторезистора, а также определять время жизни избыточных носителей заряда при разных уровнях освещенности. В отличие от традиционных методов измерения параметров фоторезисторов, работающих в динамическом режиме, в предложенной установке не используются осциллограф и отдельный модулятор светового потока (генератор или прерыватель), это позволило существенно уменьшить габаритные размеры и себестоимость комплекса, а также автоматизировать процесс измерения. Для определения частотной характеристики фоторезистора предложено использовать синтезатор частоты, который позволяет вместе с цифро-аналоговым преобразователем микроконтроллера сформировать амплитудно-модулированный световой поток требуемой частоты и глубины модуляции. Описанный комплекс может быть подключен к сети интернет при помощи Wi-Fi модуля на базе микроконтроллера ESP8266, что позволяет проводить исследования в дистанционном режиме. Также предусмотрена возможность определять параметры фоторезистора при разных значениях сопротивления нагрузки.

Ключевые слова: фоторезистор; фотопроводимость; внутренний фотоэффект; фоторезистивный эффект неравновесные носители; время жизни; люкс-амперная характеристика; микроконтроллер; синтезатор частоты.

Ил. 8. Библиогр.: 10 назв.

UDC 53.082.52

Study on inertial characteristics of photoresistors in a physical workshop / O.*M. Andreiev, O.M. Andreieva* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. № 202. P. 189 – 195.

The article describes a measuring complex based on the 32-bit STM32F103VET6 microcontroller for studying the lux-ampere (light), frequency and inertial characteristics of a photoresistor with different laws of recombination of nonequilibrium charge carriers arising under the influence of light. The developed complex is connected to a personal computer (smartphone) and allows to analyze the rise and fall edges of the photoresistor current, as well as to determine the lifetime of excess charge carriers at different illumination levels. Unlike traditional methods for measuring the pa-

rameters of photoresistors operating in a dynamic mode, the proposed measuring complex does not use an oscilloscope and a separate modulator of the luminous flux (generator or light interrupter), this made it possible to significantly reduce the size and cost of the complex, as well as automate the measurement process. To determine the frequency response of the photoresistor, it is proposed to use a frequency synthesizer, which allows, together with a digital-to-analog converter of the microcontroller, to form an amplitude-modulated light flux of the required frequency and modulation depth. The complex described in the work can be connected to the Internet using a Wi-Fi module based on an ESP8266 microcontroller, which allows conducting research in a remote mode. It is also possible to determine the parameters of the photoresistor at different values of the load resistance.

Key words: photoresistor; photoconductivity; internal photoelectric effect; photoresistive effect nonequilibrium carriers; lifetime; lux-ampere characteristic; microcontroller; frequency synthesizer.

8 fig. Ref: 10 items.