# РЕФЕРАТИ РЕФЕРАТЫ ABSTRACTS

## МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
## МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
## METHODS AND MECHANISMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

УДК 004.056.5

**Порівняльний аналіз одноразових підписів на базі геш-функцій** / *В.В. Семенець, О.С. Марухненко, І.Д. Горбенко, Г.З. Халімов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 5 – 18.

Підписи на основі геш-функцій є широким класом постквантових криптографічних алгоритмів, їх стійкість базується на складності задач пошуку колізій та прообразів для криптографічних геш-функцій. Основними перевагами цього класу є постквантовість, легка модифікація та добре досліджена математична база. До недоліків відносяться великі розміри підписів та обмежена кількість використань однієї пари ключів. До найбільш перспективних алгоритмів цього класу належать криптосистеми типу SPHINCS, які мають складну структуру, що включає, серед інших, одноразовий підпис Вінтерніца. В роботі проведено аналіз існуючих алгоритмів одноразового підпису, як широко відомих схем Лампорта та Вінтерніца з урахуванням модифікацій останнього, так і альтернативних методів. Проведено аналіз стійкості модифікованих алгоритмів, який показав, що їх стійкість базується на тій самій математичній базі, що і стійкість оригінальних алгоритмів. Вимога одноразового використання залишається критично важливою для безпеки кожного з досліджених алгоритмів. Порівняно розміри ключів та підписів та обчислювальну складність різних алгоритмів, що і складає їх основні відмінності. Модифіковані алгоритму не вносять принципово нових складових в криптосистеми але дозволяють досягти певної оптимізації, зміщуючи умови просторово-часового компромісу. Окремий інтерес представляє розширений підпис Лампорта, що має ту ж обчислювальну складність та розміри ключів, що і оригінальний алгоритм, і при цьому дозволяє вдвічі зменшити розмір підпису. В контексті криптосистеми SPHINCS підпис Вінтерніца залишається кращим варіантом, оскільки дозволяє повністю обчислювати публічний ключ безпосередньо з підпису.

*Ключові слова:* підписи на базі геш-функцій; одноразові підписи; підпис Лампорта; підпис Вінтерніца; постквантова криптографія.

Табл. 9. Бібліогр.: 13 назв.

УДК 004.056.5

**Сравнительный анализ одноразовых подписей на основе хеш-функций** / *В.В. Семенец, А.С. Марухненко, И.Д. Горбенко, Г.З. Халимов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 5 – 18.

Подписи на основе хеш-функций являются широким классом постквантовых криптографических алгоритмов, их стойкость базируется на сложности задач поиска коллизий и прообразов для криптографических хеш-функций. Основными преимуществами данного класса являются постквантовость, легкая модификация и хорошо исследованная математическая база. Недостатки – большие размеры подписей и ограниченное количество использований одной пары ключей. К наиболее перспективным алгоритмам этого класса относятся криптосистемы типа SPHINCS, которые имеют сложную структуру, включающую, среди прочих, одноразовую подпись Винтерница. В работе проведен анализ существующих алгоритмов одноразовой подписи, как широко известных схем Лампорта и Винтерница с учетом модификаций последнего, так и альтернативных методов. Проведен анализ стойкости модифицированных алгоритмов, который показал, что их безопасность базируется на той же математической базе, что и стойкость оригинальных алгоритмов. Требование одноразового использования остается критично важным для безопасности каждого из исследованных алгоритмов. Выполнено сравнение размеров ключей и подписей и вычислительной сложности различных алгоритмов, в чем и заключается их основные отличия. Модифицированные алгоритма не вносят принципиально новых составляющих в криптосистемы, но позволяют достичь определенной оптимизации, смещая условия пространственно-временного компромисса. Отдельный интерес представляет расширенная подпись Лампорта, имеющая ту же вычислительную сложность и размеры ключей, как и оригинальный алгоритм, и при этом позволяющая вдвое уменьшить размер подписи. В контексте криптосистемы SPHINCS подпись Винтерница остается лучшим вариантом, поскольку позволяет полностью вычислять публичный ключ непосредственно из подписи.

*Ключевые слова:* подписи на основе хеш-функций; одноразовые подписи; подпись Лампорта; подпись Винтерница; постквантовая криптография.

Табл. 9. Библиогр.: 13 назв.

UDC 004.056.5

**Comparative analysis of one-time hash-based signatures** / *V.V. Semenetz, O.S. Marukhnenko, I.D. Gorbenko, G.Z. Khalimov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 5 – 18.

Hash-based signatures are a wide class of post-quantum cryptographic algorithms, their security is based on the complexity of collision and preimage search problems for cryptographic hash functions. The main advantages of this class are post-quantization, easy modification and a well-researched mathematical base. The disadvantages are large sizes of signatures and limited number of uses of one key pair. The most promising algorithms of this class include algorithms of the SPHINCS type, which have a complex structure, including, among others, a one-time Winternitz signature. The paper analyzes the existing one-time signature algorithms, both well-known Lamport and Winternitz schemes, taking into account modifications of the latter one, and alternative methods. An analysis of the security of modified algorithms has been shown, which showed that their security is based on the same mathematical basis as the security of the original algorithms. The one-time use requirement remains critical to the safety of each of the algorithms studied. The sizes of keys and signatures and computational complexity of various algorithms are compared, in what their basic differences consist. The modified algorithms do not add fundamentally new components in cryptosystems but they make it possible to achieve a certain optimization, shifting the conditions of space-time compromise. The extended Lamport signature is of a particular interest, having the same computational complexity and key sizes as the original algorithm, and at the same time allowing one to halve the signature size. In the context of the SPHINCS cryptosystem, the Winternitz signature remains the best option, since it allows the complete computation of the public key directly from the signature.

*Key words:* hash-based signatures; one-time signatures; Lamport signature; Winternitz signature; post-quantum cryptography.

9 tab. Ref: 13 items.

УДК 004.056.55

**Аналіз та дослідження алгоритму цифрового підпису Picnic** / *М.В. Єсіна, Б.С. Шахов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 19 – 24.

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів NIST США обрано математичні методи цифрового підпису (ЦП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптографами та математиками на найвищому рівні. Вони детально описані та пройшли дослідження на першому етапі міжнародного конкурсу NIST США. В процесі другого етапу прийнято ряд рішень стосовно об'єднання деяких кандидатів на постквантовий стандарт ЦП. Для подальших досліджень на 2-му етапі залишили 9 кандидатів: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, Falcon, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів. За результатами досліджень перспективних постквантових криптографічних алгоритмів типу цифровий підпис протягом 2-го раунду конкурсу NIST США було отримано наступні результати – були обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів були обрані такі алгоритми ЦП: Crystals-Dilithium, Falcon та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+. У даній роботі розглядаються особливості побудови алгоритму цифрового підпису, який розглядається як кандидат на перспективний постквантовий стандарт конкурсу NIST PQC – Picnic, а також проводиться аналіз захищеності алгоритму від відомих атак. Приводяться дані з порівняння постквантових алгоритмів типу цифровий підпис. Наводиться опис алгоритму Picnic та його параметрів.

*Ключові слова:* аналіз відомих атак; блокові потокові шифри; відкритий ключ; геш-функції; ключові пари; постквантовий алгоритм Picnic; постквантова захищеність; стандарти шифрування; таємний ключ; цифровий підпис; LowMC.

Табл. 3. Бібліогр.: 7 назв.

УДК 004.056.55

**Анализ и исследование алгоритма цифровой подписи Picnic** / *М.В. Есина, Б.С. Шахов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 19 – 24.

Важной особенностью постквантового периода в криптографии является существенная неопределенность относительно исходных данных для криптоанализа и противодействия в части возможностей квантовых компьютеров, их математического и программного обеспечения, а также применение квантового криптоанализа к существующим криптопреобразованиям и криптопротоколам. В качестве основных методов NIST США избрал математические методы цифровой подписи (ЦП), прошедшие существенный анализ и обоснование в процессе широких исследований криптографами и математиками на высшем уровне. Они подробно описаны и прошли исследования на первом этапе международного конкурса NIST США. В процессе второго этапа принят ряд решений относительно объединения некоторых кандидатов на постквантовый стандарт ЦП. Для дальнейших исследований на 2-м этапе оставили 9 кандидатов: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow и SPHINCS+. Три из них (Dilithium, Falcon, qTeSLA) основаны на стойкости алгебраических решеток (Lattice-based), четыре (GeMSS, LUOV, MQDSS, Rainbow) – на основе многомерных преобразований (MQ-преобразование), один (SPHINCS+) – на стойкости хеш-функции, один (Picnic) – на стойкости хеш-функции и блочных потоковых шифров. По результатам исследований перспективных постквантовых крипто-

графических алгоритмов типа цифровая подпись в течение 2-го раунда конкурса NIST США были получены следующие результаты – выбраны алгоритмы-финалисты и альтернативные алгоритмы. В качестве алгоритмов-финалистов выбраны алгоритмы ЦП: Crystals-Dilithium, Falcon и Rainbow. В качестве альтернативных алгоритмов – GeMSS, Picnic и SPHINCS+. В данной работе рассматриваются особенности построения алгоритма цифровой подписи, который рассматривается как кандидат на перспективный постквантовый стандарт конкурса NIST PQC – Picnic, а также проводится анализ защищенности алгоритма от известных атак. Приводятся данные из сравнения постквантовых алгоритмов типа цифровая подпись. Приводится описание алгоритма Picnic и его параметров.

*Ключевые слова:* анализ известных атак; блочные поточные шифры; открытый ключ; хеш-функции; ключевые пары; постквантовый алгоритм Picnic; постквантовая защищенность; стандарты шифрования; секретный ключ; цифровая подпись; LowMC.

Табл. 3. Библиогр.: 7 назв.

UDC 004.056.55

**Analysis and research of digital signature algorithm Picnic** / *M.V. Yesina, B.S. Shahov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 19 – 24.

An important feature of the post-quantum period in cryptography is the significant uncertainty regarding the source data for cryptanalysis and counteraction in terms of the capabilities of quantum computers, their mathematical and software, as well as the application of quantum cryptanalysis to existing cryptotransformations and cryptoprotocols. Mathematical methods of digital signature (DS) have been chosen as the main methods of NIST USA, which have undergone significant analysis and substantiation in the process of extensive research by cryptographers and mathematicians at the highest level. They are described in detail and studied at the first stage of the US NIST International Competition. In the second round, a number of decisions were made to merge some candidates for the post-quantum DS standard. 9 candidates were left for further research at the 2nd round: Crystals-Dilithium, Falcon, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow and SPHINCS+. Three of them (Dilithium, Falcon, qTeSLA) are based on the stability of algebraic lattices (Lattice-based), four (GeMSS, LUOV, MQDSS, Rainbow) are based on multivariate transformations (MQ-transformations), one (SPHINCS+) is based on the stability of hash-function, one (Picnic) is based on the stability of the hash-function and block stream ciphers. During the 2nd round of the US NIST Competition the following finalist algorithms and alternative algorithms were selected as digital signatures according to the results of research on promising post-quantum cryptographic algorithms. As finalists algorithms such DS algorithms as Crystals-Dilithium, Falcon and Rainbow. Alternative algorithms are GeMSS, Picnic and SPHINCS+ were selected. This paper studies the peculiarities of construction of the digital signature algorithm considered as a candidate for the promising post-quantum standard of the NIST PQC competition – Picnic, also it analyzes the protection of the algorithm from known attacks. Data from the comparison of post-quantum algorithms such as digital signature are given. The description of the Picnic algorithm and its parameters are given.

*Key words:* analysis of known attacks; block stream ciphers; public key; hash functions; key pairs; post-quantum algorithm Picnic; post-quantum security; encryption standards; secret key; digital signature; LowMC.

3 tab. Ref: 7 items.

УДК 004.056.5

**Уточнення оцінок ймовірності успіху атаки подвійної витрати на блокчейн системи з урахуванням моделі незалежних гравців /** *М.А. Полуяненко, Ю.І. Горбенко, В.Е. Сафоненко, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 25 – 37.

Технологія блокчейн досліджується в багатьох інноваційних програмах, таких як: криптовалюта; розумні контракти; системи зв'язку; охорона здоров'я; Інтернет речі; фінансові системи; розробка програмного забезпечення; електронне голосування та багато інших. Використовуючи прозору і повністю розподілену однорангову архітектуру блокчейн, додатки виграють від моделі, в якій можливо тільки додавання даних, в якій «транзакції» приймаються в блокчейн реєстр і при правильному функціонуванні системи не можуть бути модифіковані або видалені. Прозорість блокчейн систем дозволяє зберігати загальнодоступні і незаперечні записи. Тимчасова блокчейн система забезпечує перевірене ведення реєстру без централізованого управління, що дозволяє вирішувати проблеми єдиної точки відмови і єдиної точки довіри. У статті розглядається питання безпеки застосування облікових систем, побудованих за децентралізованими принципами з використанням блокчейн технології. Особливу увагу приділяється проблемі можливості проведення подвійних витрат в таких облікових системах. Наводяться приклади реорганізації записів у блокчейн реєстрах, які були виконані за допомогою вдалого проведення атак 51 % на алгоритми консенсусу на основі Доказу виконаної роботи. Приводиться уточнення аналітичних виразів ймовірності проведення атак 51 %, отриманих в роботах С. Накамото та М. Розенфельда, коли використовували більш загальну модель – модель незалежних гравців, де ймовірність формування блоків зловмисниками та чесною мережею є незалежними подіями. Наводяться результати порівняння ймовірності успіху атаки подвійних витрат на блокчейн системи, розрахованих за різними моделями.

*Ключові слова:* атака подвійний витрати; технологія блокчейн; протоколи консенсусу; децентралізовані системи.

Іл. 3. Бібліогр.: 83 назв.

УДК 004.056.5

**Уточнение оценок вероятности успеха атаки двойной траты на блокчейн системы на основе модели независимых игроков** / *Н.А. Полуяненко, Ю.І. Горбенко, В.Э. Сафоненко, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 25 – 37.

Технология блокчейн исследуется во многих инновационных приложениях, таких как: криптовалюты; умные контракты; системы связи; здравоохранение; Интернет вещи; финансовые системы; разработка программного обеспечения; электронное голосование и многие другие. Используя прозрачную и полностью распределенную одноранговую архитектуру блокчейн, приложения выигрывают от модели, в которой возможно только добавление данных, в которой «транзакции» принимаются в блокчейн реестр и при правильном функционировании системы не могут быть модифицированы или удалены. Прозрачность блокчейн систем позволяет хранить общедоступные и неопровержимые записи. Одноранговая блокчейн система обеспечивает проверяемое ведение реестра без централизованного управления, что позволяет решать проблемы единой точки отказа и единой точки доверия. В статье рассматривается вопрос безопасности применения учетных систем, построенных децентрализованными принципами с использованием блокчейн технологии. Особое внимание уделяется проблеме проведения двойных расходов в таких учетных системах. Приводятся примеры реорганизации записей в блокчейн реестрах, которые были выполнены с помощью удачного проведения атак 51 % на алгоритмы консенсуса на основе Доказательства выполненной работы. Приводится уточнение аналитических выражений вероятности проведения атак 51 %, полученных в работах С. Накамото и М. Розенфельда, когда использовали более общую модель – модель независимых игроков, где вероятность формирования блоков злоумышленниками и честной сетью являются независимыми событиями. Приводятся результаты сравнения вероятности успеха атаки двойных расходов на блокчейн системы, рассчитанных по разным моделям.

*Ключевые слова:* атака двойной траты; технология блокчейн; протоколы консенсуса; децентрализованные системы.

Ил. 3. Библиогр.: 83 назв.

UDC 004.056.5

**Refinement of estimates of the success probability of a double-spend attack on the Blockchain System, Based on the Independent Players Model** / *N.A. Poluyanenko, Yu.I. Gorbenko, V.E. Safonenko, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. № 203. P. 25 – 37.

Blockchain technology is being studied in many innovative applications, such as: cryptocurrencies, smart contracts, communication systems, healthcare, Internet of Things, financial systems, software development, electronic voting and many others. Using a transparent and fully distributed peer-to-peer blockchain architecture, applications benefit from a data-only model, in which “transactions” are accepted into the blockchain ledger and, if the system is functioning properly, cannot be modified or deleted. The transparency of blockchain systems makes it possible to store publicly available and irrefutable records. A peer-to-peer blockchain system provides verifiable ledger maintenance without centralized management, which solves the problems of a single point of failure and a single point of trust. The article deals with the issue of the security of application of accounting systems built on decentralized principles using blockchain technology. Particular attention is paid to the problem of the possibility of double spending in such accounting systems. The article exemplifies the reorganization of records in blockchain ledgers, performed by successfully carrying out a 51% attack on consensus algorithms based on proof of work. Given refinement of analytical expressions of 51% attack probability obtained in the works of S. Nakamoto and M. Rosenfeld using a more general model, namely, the model of independent players, where the probability of block formation by attackers and an honest network are independent events. The results of comparing of the success probability of a double-spending attack on the blockchain systems calculated according to different models are presented.

*Key words:* double spend attack; blockchain technology; consensus protocols; decentralized systems.

3 fig. Ref: 83 items.

УДК 004.056.5

**Приховування даних на основі адресації шумоподібних сигналів** / *О.О. Кузнецов, О.А. Смирнов, А.С. Киян, Т.Ю. Кузнецова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 38 – 49.

Для передачі секретних повідомлень використовуються різні обчислювальні методи. Наприклад, криптографічні методи приховують смисловий зміст повідомлень, що передаються, представляючи їх у вигляді шумоподібних безглуздих даних. Стеганографічні методи приховують факт існування інформаційних повідомлень. Для цього повідомлення приховуються всередині контейнерів (cover files) – надлишкових даних, які передаються відкритим способом і не викликають ні в кого підозр. Сторонній спостерігач може перехоплювати cover files, аналізувати і досліджувати їх, проте детектувати приховані дані і тим більше їх відновлювати для нього дуже складно або взагалі неможливо. У статті обговорюються методи приховування даних у контейнерах-переносчиках з використанням технологій прямого розширення спектра. Представляється новий метод, який полягає у прямій адресації псевдовипадкових послідовностей. З одного боку це значно зменшує викривлення контейнерів-переносчиків. З іншого боку – інтенсивність помилок у відновлених повідомленнях не збільшується. Результати експериментальних досліджень показують, що за порівнянням з іншими відомими методами дійсно вдається зменшити викривлення контейнерів-переносників (в експериментах використовувались контейнери-зображення). У статті приводяться наочні приклади, а також показані переваги запропонованого методу.

Приводяться результати експериментальних досліджень за оцінкою якості зображень. Ці результати підтверджують адекватність та достовірність теоретичних оцінок.

*Ключові слова:* стеганографія з розширеним спектром; приховування даних; контейнери-зображення; пряме розширення спектру; псевдовипадкова послідовність.

Іл. 8. Бібліогр.: 37 назв.

УДК 004.056.5

**Сокрытие данных на основе адресации шумоподобных сигналов** / *А.А. Кузнецов, А.А. Смирнов, А.С. Киян, Т.Ю. Кузнецова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 38 – 49.

Для передачи секретных сообщений используются различные вычислительные методы. Например, криптографические методы скрывают смысловое содержание передаваемых сообщений, представляя их в виде шумоподобных бессмысленных данных. Стеганографические методы скрывают факт существования информационных сообщений. Для этого сообщения скрываются внутри контейнеров (cover files) – избыточных данных, которые передаются открытым способом и не вызывают ни у кого подозрений. Сторонний наблюдатель может перехватывать cover files, анализировать и исследовать их, однако детектировать сокрытые данные и тем более их восстанавливать для него очень сложно или вообще невозможно. В статье обсуждаются методы сокрытия данных в контейнерах-переносчиках с использованием технологии прямого расширения спектра. Предлагается новый метод, который заключается в прямой адресации псевдослучайных последовательностей. С одной стороны, это значительно уменьшает искажение контейнеры-переносчики. С другой стороны, интенсивность ошибок в восстановленных сообщениях не увеличивается. Результаты экспериментальных исследований показывают, что по сравнению с другими известными методами действительно удается уменьшить искажения контейнеров-переносчиков (в экспериментах использовались контейнеры-изображения). В статье приводятся наглядные примеры, а также показаны преимущества предложенного метода. Приводятся результаты экспериментальных исследований по оценке качества изображений, подтверждающие адекватность и достоверность теоретических результатов.

*Ключевые слова:* стеганография с расширенным спектром; сокрытие данных; контейнеры-изображения; прямое расширение спектра; псевдослучайная последовательность.

Ил. 8. Библиогр.: 37 назв.

UDC 004.056.5

**Data hiding based on noise-like signal addressing** / *A.A. Kuznetsov, O.A. Smirnov, A.S. Kiian, T.Y. Kuznetsova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 38 – 49.

There are various computing techniques (methods) to transmit secret messages. For example, cryptographic techniques hide the semantic content of transmitted messages, presenting them in the form of noise-like minor data. Steganographic techniques hide the existence of information messages itself. In this case, messages are hidden inside cover files, i.e., redundant data that are transmitted in an open way and do not cause suspicion in anyone. An outside observer can intercept cover files, analyze and examine them. However, it is very difficult or even impossible to detect and recover hidden data. This article discusses the techniques for hiding data in cover images using direct spread spectrum. We propose a new technique that consists in direct addressing of pseudo-random sequences. On the one hand, it significantly reduces cover file distortion. On the other hand, the error rate in recovered messages does not increase. Our experiments have shown, that Spread Spectrum Steganography technique indeed reduce the distortion in cover images compared to other techniques. We give some illustrative examples and show the advantages of the proposed method. Even with a significant increase in encoding density, the quality of cover images does not degrade. We also conduct experiments and evaluate image quality based on Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The obtained results of experimental studies confirm the adequacy and reliability of the research results. The main disadvantage of the proposed data hiding technique is a high computational complexity. To recover messages, it is necessary to calculate sequentially the correlation coefficients with a large number of pseudo-random sequences.

*Key words:* Spread Spectrum Steganographic; Data Hiding; cover images; direct spread spectrum; pseudo-random sequence

8 fig. Ref: 37 items.

УДК 621.391.15:519.7

**Оцінка ефективності диференціального додавання точок кривих в узагальненій формі Едвардса** / *А.В. Бессалов, Л.В. Ковальчук, Н.В. Кучинська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 50 – 59.

Дано огляд основних властивостей трьох класів кривих в узагальненій формі Едвардса: повних, квадратичних і скручених кривих Едвардса. Проведено аналіз алгоритму Монтгомері диференціального додавання точок для кривої в формі Монтгомері. Наведено оцінку рекордно малої вартості обчислення скалярного добутку $kP$ точки $P$, яка дорівнює $5M+4S+1U$ на одному кроці ітеративного циклу ($M$ – вартість операції обчислення добутку в скінченному полі, $S$ – вартість піднесення до квадрату, $U$ – вартість множення на відому константу). Дано ретельний вивід формул додавання-віднімання і подвоєння точок для кривої в узагальненій формі Едвардса в проективних координатах Фарашахи – Хоссейни. Перехід від тривимірних проективних координат

$(X:Y:Z)$ до двовимірних координат $(W:Z)$ дозволяє для кривих Едвардса досягти тієї ж самої мінімальної вартості обчислень $5M+4S+1U$, що і для кривої в формі Монтгомері. Обговорюються аспекти вибору придатної для криптографії кривої в формі Едвардса і оптимізації її параметрів в задачі диференціального додавання точок. Рекомендуються скручені криві Едвардса порядку $N_E = 4n$ ($n$ - просте) при $p \equiv 5 \bmod 8$, для яких мінімізація параметрів $a$ та $d$ дозволяє досягнути мінімальної оцінки вартості $5M+4S$ для одного кроку обчислення скалярного добутку точки. Показано, що перехід від кривих в формі Вейерштраса, які використовуються в сучасних криптографічних стандартах, до кривих в формі Едвардса, дозволяє отримати потенціальний виграш в швидкості обчислення скалярного добутку точки в 3,09 рази.

*Ключові слова:* крива в узагальненій формі Едвардса; повна крива Едвардса; скручена крива Едвардса; квадратична крива Едвардса; порядок кривої; порядок точки; ізоморфізм; диференціальне додавання; вартість обчислень; квадратичний лишок; квадратичний нелишок.

Бібліогр.: 10 назв.

УДК 621.391.15:519.7

**Оценка эффективности дифференциального сложения точек кривых в обобщенной форме Эдвардса** / *А.В. Бессалов, Л.В. Ковальчук, Н.В. Кучинская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 50 – 59.

Дан обзор основных свойств трех классов кривых в обобщенной форме Эдвардса: полных, квадратичных и скрученных кривых Эдвардса. Проведен анализ алгоритма Монтгомери дифференциального сложения точек для кривой в форме Монтгомери. Приведена оценка рекордно малой стоимости вычисления скалярного произведения $kP$ точки $P$, равная $5M+4S+1U$ на одном шаге итеративного цикла ($M$ – стоимость вычисления умножения в конечном поле, $S$ - стоимость возведения в квадрат, $U$ – стоимость умножения на известную константу). Приведен подробный вывод формул сложения-вычитания и удвоения точек для кривой в обобщенной форме Эдвардса в проективных координатах Фарашахи – Хоссейни. Переход от трехмерных проективных координат $(X:Y:Z)$ к двухмерным координатам $(W:Z)$ позволяет для кривых Эдвардса достичь той же минимальной стоимости вычислений $5M+4S+1U$, что и для кривой в форме Монтгомери. Обсуждаются аспекты выбора приемлемой для криптографии кривой в форме Эдвардса и оптимизации ее параметров в задаче дифференциального сложения точек. Рекомендуются скрученные кривые Эдвардса с порядком $N_E = 4n$ ($n$ - простое) при $p \equiv 5 \bmod 8$, минимизация параметров $a$ и $d$ которых позволяет достичь минимальной оценки стоимости $5M+4S$ одного шага вычисления скалярного произведения точки. Показано, что переход от используемых в современных стандартах кривых в форме Вейерштрасса к кривым в форме Эдвардса позволяет получить потенциальный выигрыш в скорости вычисления скалярного произведения точки в 3,09 раза.

*Ключевые слова:* кривая в обобщенной форме Эдвардса; полная кривая Эдвардса; скрученная кривая Эдвардса; квадратичная кривая Эдвардса; порядок кривой; порядок точки; изоморфизм; дифференциальное сложение; стоимость вычислений; квадратичный вычет; квадратичный невычет.

Библиогр.: 10 назв.

UDC 621.391.15:519.7

**Evaluation of the efficiency of differential addition of points of curves in the generalized Edwards form** / *A.V. Bessalov, L.V. Kovalchuk, N.V. Kuchynska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 50 – 59.

A survey of the main properties of three classes of curves in the generalized Edwards form is given: complete, quadratic and twisted Edwards curves. The analysis of the Montgomery algorithm for differential addition of points for the Montgomery curve is carried out. An estimation of the record low cost of computing the scalar product $kP$ of a point $P$ is given, which is equal to $5M+4S+1U$ on one step of the iterative cycle ($M$ is the cost of finite field multiplication, $S$ is the cost of squaring, $U$ is the cost of field multiplication by a known constant). A detailed derivation of the formulas for addition-subtraction and doubling point s for the curve in the generalized Edwards form in projective coordinates of Farashahi-Hosseini is carried out. Moving from three-dimensional projective coordinates *(X: Y: Z)* to two-dimensional coordinates *(W: Z)* allows achieving the same minimum computational cost for the Edwards curves as for the Montgomery curve. Aspects of the choice of an Edwards-form curve acceptable for cryptography and its parameters optimization in the problem of differential addition of points are discussed. Twisted Edwards curves with the order of $N_E = 4n$ ($n$ is prime) are recommended, minimizing the parameters $a$ and $d$ allows achieving the minimum cost estimation $5M+4S$ for one step of computing the point product. It is shown that the transition from the Weierstrass curves (the form used in modern cryptographic standards) to the Edwards curves makes it possible to obtain a potential gain in the speed of computing the scalar product of the point by a factor of 3.09.

*Key words:* Edwards curve in generalized form; complete Edwards curve; twisted Edwards curve; quadratic Edwards curve; curves order; points order; isomorphism; differential addition; computing cost; square; non square.

Ref: 10 items.

УДК 004.056.55

**Постквантовий алгоритм інкапсуляції ключів Classic McEliece /** *М.С. Луценко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 60 – 81.

Проводиться комплексний аналіз кандидата-фіналіста міжнародного конкурсу постквантової криптографії NIST PQC, а саме – алгоритму інкапсуляції ключів на основі кодових криптосистем Classic McEliece. Метою роботи є первинне дослідження базових характеристик алгоритму Classic McEliece, таких як математична модель, очікувана криптографічна стійкість і кількісна оцінка витрачених ресурсів.

Проводиться аналіз математичної моделі алгоритму Classic McEliece, наводиться опис основних функцій і перетворень, порівняння первинної моделі алгоритму, запропонованого Робертом Мак-Елісом в 1978 р., і алгоритму, що розглядається, аналіз внесених авторами Classic McEliece модифікацій. Також наводяться рекомендації щодо подальших напрямків досліджень і доробок алгоритму.

В якості первинної оцінки криптографічної стійкості проведений аналіз відповідності сучасним вимогам до постквантових криптосистем, а саме – властивості нерозрізненості для атак на основі підібраного відкритого тексту, нерозрізненості для неадаптивних і адаптивних атак на основі підібраного шифротесту.

Проводиться аналіз витрат пам'яті на зберігання системних параметрів, оцінка впливу їх розміру на швидкодію системи. Також проводиться порівняння характеристик алгоритму Classic McEliece з подібними алгоритмами на основі алгебраїчних кодів, які були представлені в якості альтернативних варіантів на конкурсі NIST PQC, а саме алгоритмами BIKE і HQC. Оцінка швидкодії проводиться для трьох базових функцій алгоритму: генерації ключів, інкапсуляції і деінкапсуляції.

*Ключові слова:* криптосистеми з відкритим ключем; криптосистеми на основі алгебраїчних кодів; пост квантова криптографія; інкапсуляція ключів; швидкодія.

Табл. 4. Іл. 9. Бібліогр.: 15 назв.

УДК 004.056.55

**Постквантовый алгоритм инкапсуляции ключей Classic McEliece /** *М.С. Луценко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 60 – 81.

Проводится комплексный анализ кандидата-финалиста международного конкурса постквантовой криптографии NIST PQC, а именно – алгоритма инкапсуляции ключей на основе кодовых криптосистем Classic McEliece. Целью работы – первичное исследование базовых характеристик алгоритма Classic McEliece, таких как математическая модель, ожидаемая криптографическая стойкость и количественная оценка затрачиваемых ресурсов.

Проводится анализ математической модели алгоритма Classic McEliece, приводится описание основных функций и преобразований, сравнение первичной модели алгоритма, предложенного Робертом Мак-Элисом в 1978 г., и рассматриваемого алгоритма, анализ внесенных авторами Classic McEliece модификаций. Также приводятся рекомендации по дальнейшим направлениям исследований и доработок алгоритма.

В качестве первичной оценки криптографической стойкости проведен анализ соответствия современным требования к постквантовым криптосистемам, а именно – обеспечение свойства неразличимости для атак на основе подобранного открытого текста, неразличимость для неадаптивных и адаптивных атак на основе подобранного шифротекста.

В работе проводится анализ затрат памяти на хранение системных параметров, оценка влияния их размера на быстродействие системы. Также проводится сравнение характеристик алгоритма Classic McEliece с подобными алгоритмами на основе алгебраических кодов, которые были представлены в качестве альтернативных вариантов на конкурсе NIST PQC, а именно – алгоритмами BIKE и HQC. Оценка быстродействия проводится для трех базовых функций алгоритма: генерации ключей, инкапсуляции и деинкапсуляции.

*Ключевые слова:* криптосистемы с открытым ключом; криптосистемы на основе алгебраических кодов; пост квантовая криптография; инкапсуляция ключей; быстродействие.

Табл. 4. Ил. 9. Библиогр.: 15 назв.

UDC 004.056.55

**Post-quantum algorithm of Classic McEliece key encapsulation** / *M.S. Lutsenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 60 – 81.

A comprehensive analysis of a candidate-finalist of the International Post-quantum Cryptography Competition NIST PQC, namely, the Classic McEliece algorithm, the key encapsulation algorithm based on code cryptosystems, is carried out. The aim of this work is a primary study of the basic characteristics of the Classic McEliece algorithm, such as the mathematical model, the expected cryptographic strength and quantitative assessment of the resources.

The paper gives the analysis of the mathematical model of the Classic McEliece algorithm, description of the main functions and transformations, comparison of the primary model of the algorithm proposed by Robert McEliece in 1978 with the considered algorithm, analysis of the modifications made by the authors of Classic McEliece. It also provides recommendations for further areas of research and refinement of the algorithm. As a primary assessment of cryptographic security, an analysis of compliance with modern requirements for post-quantum cryptosystems is carried out, namely, ensuring the property of indistinguishability for attacks based on selected plaintext, indistinguishability for non-adaptive and adaptive attacks based on selected cipher text.

The paper analyzes the memory costs for storing system parameters, evaluating the impact of their size on the system performance. The characteristics of the Classic McEliece algorithm are compared with similar algorithms based on

the algebraic codes presented as alternatives at the NIST PQC Competition, namely, the BIKE and HQC algorithms. The performance evaluation is carried out for three basic functions of the algorithm: keys generation, encapsulation and de-encapsulation.

*Key words:* public key cryptosystems; cryptosystems based on algebraic codes; post-quantum cryptography; key encapsulation; performance.

4 tab. 9 fig. Ref: 15 items.

УДК 003.026:004.056

**Проект стандарту електронного підпису Rainbow та його основні властивості і можливості щодо застосування** / *Д.В. Гармаш, Г.А. Малєєва, С.О. Кандій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 82 – 90.

За результатами другого етапу міжнародного конкурсу щодо проведення досліджень та розробки стандартів асиметричних криптографічних перетворень постквантового періоду позитивну оцінку та визнання фіналістом отримав механізм електронного підпису (ЕП) Rainbow. Його важливими перевагами, у порівнянні з іншими постквантовими ЕП є менша складність прямого та зворотного перетворень – вироблення та перевірки підпису, а також суттєво зменшена довжина підпису. Разом з тим довжина відкритого ключа у нього достатньо велика. Тому є думка, що Rainbow не підходить як алгоритм ЕП загального призначення для заміни алгоритмів, які наразі визначені у FIPS 186-4. Зокрема, великі відкриті ключі роблять ланцюги сертифікатів надзвичайно великими. Однак є додатки, яким не потрібно надто часто надсилати ключі, тому цей недолік у цих випадках може бути несуттєвим. За цих умов механізм ЕП Rainbow може знайти застосування, в тому числі збільшуючи різноманітність постквантових ЕП. Також, суттєво проблемним є обмеження рівнів безпеки ЕП Rainbow 256 біт проти класичного та 128 біт проти квантового криптоаналізу.

Предметом статті є аналіз та узагальнення конструкцій механізму Oil-Vinegar систем автентифікації з відкритим ключем на основі застосування ЕП Rainbow. Це важливий напрямок щодо створення безпечних та ефективних систем автентифікації для практичних застосувань з використанням відкритих ключів, наприклад недорогих смарт-карт, коли потрібна швидкодія при виробленні та перевірці ЕП. Особливістю такого механізму автентифікації є реалізація ідеї багаторівневої системи Oil-Vinegar. Вважається, що система автентифікації на основі ЕП повинна бути більш безпечною у змісті криптографічної стійкості та більш ефективною у змісті широкого застосування у малопотужних тощо додатках. Важливість вирішення цієї проблемної задачі полягає у потенційному застосуванні механізму Rainbow, як надійно безпечної та дуже ефективної системи автентифікації з відкритим ключем на основі ЕП.

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

Табл. 1. Бібліогр.: 8 назв.

УДК 003.026:004.056

**Проект стандарта электронной подписи Rainbow и его основные свойства и возможности применения** / *Д.В. Гармаш, Г.А. Малеева, С.О. Кандий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 82 – 90.

По результатам второго этапа международного конкурса по проведению исследований и разработки стандартов асимметричных криптографических преобразований постквантового периода положительную оценку и признание финалистом получил механизм электронной подписи (ЭП) Rainbow. Его важными преимуществами по сравнению с другими постквантовыми ЭП, это меньше сложность прямого и обратного преобразований – выработка и проверки подписи, а также существенно уменьшена длина подписи. Вместе с тем длина открытого ключа у него достаточно велика. Поэтому есть мнение, что Rainbow не подходит как алгоритм ЭП общего назначения для замены алгоритмов, которые сейчас определены в FIPS 186-4. В частности, большие открытые ключи делают цепи сертификатов чрезвычайно большими. Однако есть приложения, которым не нужно слишком часто посылать ключи, поэтому этот недостаток в этих случаях может быть несущественным. В этих условиях механизм ЭП Rainbow может найти применение, в том числе увеличивая разнообразие постквантовых ЭП. Также, существенно проблемным является ограничение уровней безопасности ЭП Rainbow 256 бит против классического и 128 бит против квантового криптоанализа.

Предметом статьи является анализ и обобщение конструкций механизма Oil-Vinegar систем аутентификации с открытым ключом на основе применения ЭП Rainbow. Это важное направление по созданию безопасных и эффективных систем аутентификации для практических приложений с использованием открытых ключей, например недорогих смарт-карт, когда требуется быстродействие при выработке и проверке ЭП. Особенностью такого механизма аутентификации является реализация идеи многоуровневой системы Oil-Vinegar. Считается, что система аутентификации на основе ЭП должна быть более безопасной в смысле криптографической стойкости и более эффективной в смысле широкого применения в маломощных т.д. приложениях. Важность решения этой проблемной задачи заключается в потенциальном применении механизма Rainbow, как надежно безопасной и очень эффективной системы аутентификации с открытым ключом на основе ЭП.

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

Табл. 1. Библиогр.: 8 назв.

UDC 003.026:004.056

**Draft of Rainbow electronic signature standard and its main properties and application possibilities** / *D.V. Garmash, G.A. Maleeva, S.O. Kandiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 82 – 90.

According to the results of the second stage of the international competition for research and development of standards for asymmetric cryptographic transformations of the post-quantum period, the Rainbow electronic signature (ES) mechanism received a positive assessment and recognition as a finalist. Its important advantages over other post-quantum ESs consist in less complexity of direct and inverse transformations, i.e., signature generation and verification, as well as significantly reduced signature length. At the same time, the length of its public key is quite large. Therefore, it is thought that Rainbow is not suitable as a general-purpose ES algorithm to replace the algorithms currently defined in FIPS 186-4. In particular, large public keys make certificate chains extremely large. However, there are applications that do not need to send keys too often, so this disadvantage in these cases may be insignificant. Under these conditions, the Rainbow ES mechanism can find application, including that one increasing the diversity of postquantum ESs. Also, it is significantly problematic to limit the security levels of Rainbow ES 256 bits against classical and 128 bits against quantum cryptanalysis.

The subject of this article is the analysis and generalization of designs of the Oil-Vinegar public key authentication systems mechanism based on the Rainbow ES use. This is an important direction in creating secure and efficient authentication systems for practical applications using public keys, such as inexpensive smart cards, when speed is required in the production and verification of ES. A feature of such authentication mechanism is the implementation of the idea of a multilevel Oil-Vinegar system. It is believed that the ES-based authentication system should be more secure in terms of cryptographic stability and more efficient in terms of widespread use in low-power, etc. applications. The importance of solving this problem lies in the potential use of the Rainbow mechanism as a secure and highly efficient public-key authentication system based on ES.

*Key words:* classical and quantum cryptanalysis; threat model when using ES; list of ES threats; postquantum period.

1 tab. Ref: 8 items.

## МЕТОДИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ
## МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ
## INFORMATION PROTECTION METHODS AND MECHANISMS

УДК 004.056.52

**Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах** / *Р.Ю. Гвоздьов, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 91 – 96.

Метою статті є розробка методики формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах. На даний момент не існує методик для формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, тому розробка такої методики є актуальною задачею. В статті розглядаються методи формалізованого моделювання політики безпеки інформації та методи формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації. Обґрунтовується необхідність формального проектування комплексної системи захисту інформації та описуються вимоги при розробці формальних описів комплексної системи захисту інформації згідно з нормативними документами в сфері технічного захисту інформації. Наводиться порівняльна характеристика методів формалізованого моделювання політики безпеки інформації та методів формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації. В результаті порівняння пропонується використовувати метод UML для формального опису інформаційно-телекомунікаційної системи, а метод UMLsec – для моделювання політики безпеки. Пропонується алгоритм формування комплексу засобів захисту в інформаційно-телекомунікаційній системі з формальної моделі політики безпеки та з формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації.

*Ключові слова:* комплексна система захисту інформації; інформаційно-телекомунікаційна система; формальне проектування; Ponder; UML; UMLsec.

Табл. 3. Бібліогр.: 3 назв.

УДК 004.056.52

**Метод и методика формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах** / *Р.Ю. Гвоздев, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 91 – 96.

Целью статьи является разработка методики формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах. На данный момент не существует методик для формального проектирования комплексной системы защиты информации в информационно-телекоммуникационных системах, поэтому разработка такой методики является актуальной задачей. В статье рассматриваются методы формализованного моделирования политики безопасности информации и методы

формализованного описания информационно-телекоммуникационной системы и процессов обработки информации. Обосновывается необходимость формального проектирования комплексной системы защиты информации и описываются требования при разработке формальных описаний комплексной системы защиты информации в соответствии с нормативными документами в сфере технической защиты информации. Приводится сравнительная характеристика методов формализованного моделирования политики безопасности информации и методов формализованного описания информационно-телекоммуникационной системы и процессов обработки информации. В результате сравнения предлагается использовать метод UML для формального описания информационно-телекоммуникационной системы, а метод UMLsec – для моделирования политики безопасности. Предлагается алгоритм формирования комплекса средств защиты в информационно-телекоммуникационной системе с формальной модели политики безопасности и с формализованного описания информационно-телекоммуникационной системы и процессов обработки информации.

*Ключевые слова:* комплексная система защиты информации; информационно-телекоммуникационная система; Ponder; UML; UMLsec.

Табл. 3. Библиогр.: 3 назв.

UDC 004.056.52

**Method and technique of formal design of complex information security system in information and telecommunication systems** / *R.Y. Gvozdov, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 91 – 96.

The aim of the article is to develop a methodology for the formal design of the complex information security system in information and telecommunication systems. At the moment, there are no methods for the formal design of complex information security system in information and telecommunication systems, so the development of such a methodology is an urgent task. The article discusses the methods of formalized modeling of information security policy and methods of formalized description of the information and telecommunications system and information processing processes. The necessity of formal design of complex information security system is substantiated and the requirements for the development of formal descriptions of an integrated information security system in accordance with regulatory documents in the field of technical protection of information are described. The comparative characteristics of the methods of formalized modeling of information security policy and methods of formalized description of the information and telecommunication system and information processing processes are given. As a result of the comparison, it is proposed to use the UML method for the formal description of the information-telecommunication system, and the UMLsec method for the security policy modeling. An algorithm for the formation of a complex of protection facilities in an information and telecommunications system is proposed from a formal model of security policy and from a formalized description of an information and telecommunications system and information processing processes.

*Key words:* complex information security system; information and telecommunication system, Ponder; UML; UMLsec.

3 tab. Ref: 3 items.

УДК 681.3.06:519.248.681

**Використання BLOCKCHAIN в автомобільній безпеці** / *І.Д. Горбенко, Д.О. Фесенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 97 – 108.

Проведено аналіз проблематики використання систем автентифікації для автомобільних систем. Показано, що сучасними системами захисту автомобілів все більше цікавляться зловмисники. Автомобілі стають більш технологічними, це в свою чергу відкриває нові можливості компрометації роботи вузлів та систем автомобіля, тому до систем безпеки пред'являються все більш жорсткі вимоги щодо забезпечення ефективності та безпечності їх функціонування. Розглянуті сучасні системи захисту від незаконного заволодіння автотранспортом, більш відомі всім як «сигналізація», намагаються стримувати атаки зловмисників, але в свою чергу можуть привносити додаткові бекдори для зловмисників зовсім ненавмисно, наприклад додаючи цікаву функцію в систему автомобіля, а згодом ця функція може мати двояке значення через проблеми з системою автентифікації. Тож, виходячи з цього, системи безпеки автомобіля повинні мати найвищий рівень безпеки автентифікації, для реалізації якого пропонується використання децентралізованої мережі блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово, це дозволить відійти від стандартної клієнт-серверної архітектури, що є недостатньо захищеною. Основними шляхами вирішення зазначеної проблеми є побудування комплексної системи безпеки, що в свою чергу включає покращений та надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних схем оновлення системи передачі критичних даних автомобіля – мережі CAN. Використання даних систем дозволить поліпшити показники захищеності системи автентифікації та інформації, що курсує між блоками критичної важливості, що покращить безпечність автомобіля як від угонів, так і від можливостей створення зловмисниками аварійних ситуацій дистанційно.

*Ключові слова:* blockchain; атака; вразливість; децентралізація; підміна; automotive security.

Іл. 3. Бібліогр.: 4 назв.

УДК 681.3.06:519.248.681

**Использование BLOCKCHAIN в автомобильной безопасности** / *И.Д. Горбенко, Д.А. Фесенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 97 – 108.

Проведен анализ проблематики использования систем аутентификации для автомобильных систем. Показано, что злоумышленники все больше интересуются современными системами защиты автомобилей. Автомобили становятся более технологичными, это в свою очередь открывает новые возможности компрометации работы узлов и систем автомобиля, поэтому к системам безопасности предъявляются все более жесткие требования по обеспечению эффективности и безопасности их функционирования. Рассмотрены современные системы защиты от незаконного завладения автотранспортом, более известные всем как «сигнализация» пытаются сдерживать атаки злоумышленников, но в свою очередь могут привносить дополнительные бэкдоры для злоумышленников совершенно непреднамеренно, например, добавляя интересную функцию в систему автомобиля, а затем эта функция может иметь двоякое значение из-за проблем с системой аутентификации. Поэтому, исходя из этого, системы безопасности автомобиля должны иметь высокий уровень безопасности аутентификации, для реализации которого предлагается использовать децентрализованную сеть блокчейн с узлами для каждого автомобиля. Это позволит отойти от стандартной клиент-серверной архитектуры, которая является недостаточно защищенной. Использование данных систем позволит улучшить показатели защищенности системы аутентификации и информации, курсирующий между блоками критической важности, улучшит безопасность автомобиля как от угонов, так и от возможностей создания злоумышленниками аварийных ситуаций дистанционно.

*Ключевые слова:* blockchain; атака; уязвимость; децентрализация; подмена; automotive security.

Ил. 3. Библиогр.: 4 назв.

UDC 681.3.06:519.248.681

**Using BLOCKCHAIN in automotive security** / *I.D. Gorbenko, D. Fesenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 97 – 108.

The analysis of problems of using authentication systems for automobile systems is carried out. It is shown that criminals are increasingly interested in modern car protection systems, cars are becoming more technological, which in turn opens up new opportunities for compromising the operation of vehicle components and systems, so security systems are increasingly required to ensure efficiency and safety. Modern systems of protection against illegal seizure of vehicles, better known as "alarms" try to deter attacks by intruders, but in turn can bring additional backdoors for intruders completely unintentionally, for example by adding an interesting feature to the car system, and then this feature can be dual due to problems with the authentication system. Therefore, based on this, car security systems must have the highest level of authentication security, which requires the use of a decentralized blockchain network with nodes for each car, authenticating the user in groups, this will move away from the standard client-server architecture, which is not sufficiently secure. . The main ways to solve this problem are to build a comprehensive security system, which in turn includes an improved and reliable authentication measure based on a decentralized blockchain network and two comprehensive schemes to update the critical data transmission system of the car – CAN network. The use of these systems will improve the security of the identification system and information flowing between critical units, which will improve the safety of the car from theft, as well as from the ability of attackers to create emergencies remotely.

*Key words:* blockchain; attack; vurlerability; decentralization; substitute; automotive security

3 fig. Ref: 4 items.

УДК 004.056.5

**Дослідження властивостей носіїв інформації для стеганографічного приховування даних в кластерних файлових системах /** *К.Ю. Шеханін, Ю.І. Горбенко, Л.О. Горбачова, О.О. Кузнецов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 109 – 120.

Останніми роками набули розвитку методи технічної стеганографії. В таких системах приховування інформації досягається шляхом використання властивостей, які штучно зроблено людиною при побудові різних технічних засобів. Прикладом технічної стеганографії є застосування особливостей побудови кластерних файлових систем. Вони дозволяють ефективно приховувати інформацію шляхом зміни чергування окремих кластерів т.з. покрівельних файлів. Імена (назви) таких файлів є ключовою інформацією, і відновити приховуване повідомлення без назв покрівельних файлів вкрай важко. У роботі описано та проаналізовано різні сучасні технології збереження інформації, а саме HDD, Flash-USB, SSD. Проаналізовано кількість реалізованої продукції, ціна, швидкість зчитування та запису. Також проаналізовано важливі показники ефективності носіїв інформації з точки зору стеганографічних методів приховування інформації у кластерних файлових системах. Наприклад, досліджено швидкість послідовного зчитування/запису та швидкість доступу до випадкового кластеру, що відповідає швидкості доступу до фрагментованного файлу. Для цього використовувалися результати тестувань з ресурсу UserBenchmark. Тестування виконувалися методами Sequential та Random4k. Як висновок надана оцінка носіїв інформації та надано рекомендації щодо використання носія інформації та методу приховування даних шляхом перемішування кластерів у структурі файлової системи.

*Ключові слова:* файлові носії інформації; фрагментація; швидкість доступу; приховування даних; стеганографія

Табл. 5. Іл. 4. Бібліогр.: 39 назв.

УДК 004.056.5

**Исследование свойств носителей информации для стеганографического сокрытия данных в кластерных файловых системах /** *К.Ю. Шеханин, Ю.І. Горбенко, Л.О. Горбачова, А.А. Кузнецов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 109 – 120.

В последние годы получили развитие методы технической стеганографии. В таких системах сокрытие информации достигается путем использования свойств, искусственно созданных человеком при построении различных технических средств. Примером технической стеганографии является применение особенностей построения кластерных файловых систем. Это позволяет эффективно скрывать информацию путем изменения чередования отдельных кластеров т.н. кровельных файлов. Имена (названия) таких файлов являются ключевой информацией, и восстановить скрываемое сообщение без названий кровельных файлов крайне трудно. В работе описаны и проанализированы различные современные технологии хранения информации, а именно HDD, Flash-USB, SSD. Проанализированы количество реализованной продукции, цена, скорость считывания и записи. Также проанализированы важные показатели эффективности носителей информации с точки зрения стеганографических методов сокрытия информации в кластерных файловых системах. Например, исследованы скорость последовательного чтения/записи и скорость доступа к случайному кластера, соответствующая скорость доступа к фрагментованному файлу. Для этого использовались результаты тестирования с ресурса UserBenchmark. Тестирование выполнялись методами Sequential и Random4k. Как вывод дана оценка носителей информации и даны рекомендации по использованию метода сокрытия данных путем перемешивания кластеров в структуре файловой системы.

*Ключевые слова:* файловые носители информации; фрагментация; скорость доступа; сокрытие данных; стеганография

Табл. 5. Ил. 4. Библиогр.: 39 назв.

UDC 004.056.5

**Study of storage devices properties for steganographic data hiding in cluster file systems** / *K.Yu. Shekhanin, Yu.I. Gorbenko, L.O. Gorbachova, A.A. Kuznetsov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 109 – 120.

Methods for technical steganography have been developed in recent years. Hiding of information in such systems is achieved by using properties artificially created by human while constructing various technical means. An example of technical steganography is the application of the features of constructing clustered file systems. This makes it possible to hide information effectively by changing the alternation of individual clusters, the so-called cover files. The names of such files are the key information and it is extremely difficult to recover a hidden message without links (i.e. without names) of cover files. This work describes and analyzes various modern information storage technologies, namely HDD, Flash-USB, SSD. We have analyzed different indicators such as the number of implemented products, price, speed of reading and writing. The important indicators of storage media efficiency with regard to steganographic methods of hiding information in cluster file systems were also analyzed. For example, we have investigated the speed of sequential reading / writing and the speed of access to a random cluster that is similar to the speed of access to a fragmented file. For this, we used the test results from the UserBenchmark resource. Tests were performed using Sequential and Random4k methods. In conclusion, an assessment of information carriers is given and recommendations are given on using the method of hiding data by mixing clusters in the structure of the file system.

Key words: File storage media; fragmentation; speed of access; data hiding; steganographic

5 tab. 4 fig. Ref: 39 items.

УДК 004.056.52

**Менеджмент вразливостей з використанням формалізованого опису /** *В.О. Поддубний, О.В. Сєверінов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 121 – 125.

Розглядаються основні етапи менеджменту вразливостей та проблеми, які виникають при оцінці ризиків й прийнятті рішень під час менеджменту вразливостей в інформаційно-телекомунікаційній системі. Здійснюється припущення, що сучасні методики не є достатніми для ефективного менеджменту вразливостей. Висувається необхідність створення системи оцінювання ризиків для покращення процедур прийняття рішень. Здійснюється порівняння формалізованого та неформалізованого опису інформаційно-телекомунікаційної системи. Як результатом такого порівняння є висновок, що формалізований опис має низку переваг, тому створювана система повинна бути саме формалізованою, а для цього необхідно щоб вона була побудована на базі формалізованого опису інформаційно-телекомунікаційної системи. При додаванні якісного оцінювання вразливостей (наприклад оцінок вразливостей згідно з Common Vulnerability Scoring System) ця система матиме однозначність трактування, буде чіткою, гнучкою та простою в використанні. Додатковою перевагою такої системи є можливість автоматизації процесів оцінки та прийняття рішень, що дозволить виключити людський вплив та мінімізувати суб'єктивний фактор під час менеджменту вразливостей в інформаційно-телекомунікаційній системі. Така система не виключить вплив адміністратора безпеки та аудиту, проте допоможе йому в прийнятті рішень, оцінці ризиків, зменшить вірогідність помилок, допоможе новому персоналу під час вибору рішень.

*Ключові слова:* вразливості; система менеджменту вразливостями; СУІБ; формалізований опис ІТС; якісне оцінювання вразливостей; NVD; CVSS.

Іл. 2. Бібліогр.: 10 назв.

УДК 004.056.52

**Менеджмент уязвимостей с использованием формализованного описания** / *В.А. Поддубный, О.В. Северинов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 121 – 125.

Рассматриваются основные этапы менеджмента уязвимостей и проблемы, которые возникают при оценке рисков и принятии решений во время управления уязвимостей в информационно-телекоммуникационной системе. Осуществляется предположение, что современные методики не являются достаточными для эффективного менеджмента уязвимостей. Выдвигается необходимость создания системы оценки рисков для улучшения процедур принятия решений. Осуществляется сравнение формализованного и неформализованного описания информационно-телекоммуникационной системы. Как результат такого сравнения сделан вывод, что формализованное описание имеет ряд преимуществ, поэтому создаваемая система должна быть именно формализованной, а для этого необходимо, чтобы она была построена на базе формализованного описания информационно-телекоммуникационной системы. При добавлении качественной оценки уязвимостей (например, оценок уязвимостей согласно Common Vulnerability Scoring System) эта система будет иметь однозначность трактовки, будет четкой, гибкой и простой в использовании. Дополнительным преимуществом такой системы является возможность автоматизации процессов оценки и принятия решений, что позволит исключить человеческое влияние и минимизировать субъективный фактор при менеджменте уязвимостей в информационно-телекоммуникационной системе. Такая система не исключит влияние администратора безопасности и аудита, однако поможет ему в принятии решений, оценке рисков, уменьшит вероятность ошибок, поможет новому персоналу во время выбора решений.

*Ключевые слова:* уязвимости; система менеджмента уязвимостями; СУИБ; формализованное описание ИТС; качественное оценивание уязвимостей; NVD; CVSS.

Ил. 2. Библиогр.: 10 назв.

UDC 004.056.52

**Vulnerability management using a formalized description** / *V.O. Poddubnyi, O.B. Severinov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 121 – 125.

The article considers the main stages of vulnerability management and the problems arising in risk assessment and decision making during vulnerability management in the information and telecommunications system. It is assumed that modern techniques are not sufficient for effective vulnerability management. There is a need for creating a risk assessment system to improve decision-making procedures. The comparison of the formalized and informal description of the information and telecommunication system is described. The conclusion from the comparison results is that the formalized description has a number of advantages, so it is necessary that it should be built based on a formalized description of the information and telecommunication system. When adding qualitative vulnerability assessments (such as Common Vulnerability Scoring System vulnerabilities), this system will be unambiguous, clear, flexible, and easy to use. An additional advantage of such a system is the ability to automate assessment and decision-making processes, which will eliminate human influence and minimize the subjective factor in the management of vulnerabilities in the information and telecommunications system. Such a system will not exclude the influence of the security administrator, but will help him in decision-making, risk assessment, reduce the likelihood of errors, will help new staff in choosing decisions.

*Key words:* vulnerabilities; vulnerability management system; ISMS; formalized description of ITS; qualitative assessment of vulnerabilities; NVD; CVSS.

2 fig. Ref: 10 items.

## МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ СИГНАЛІВ
## МЕТОДЫ СИНТЕЗА И АНАЛИЗА СИГНАЛОВ
## METHODS OF SYNTHESIS AND ANALYSIS OF SIGNALS

УДК 621.391

**Методи синтезу і формування систем нелінійних дискретних сигналів для сучасних інформаційно-комунікаційних систем** / *І.Д. Горбенко, О.А. Замула, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 126 – 132.

Наведено результати вирішення актуальної проблеми поліпшення показників ефективності функціонування інформаційно-комунікаційних систем (ІКС), зокрема інформаційної безпеки, завадостійкості, скритності, швидкості формування і обробки інформації. Використовувані методи формування та обробки даних, а також класи широкосмугових сигналів, які застосовуються як фізичний переносник даних, не дозволяють забезпечити необхідні (особливо для об’єктів критичної інфраструктури) показники інформаційної безпеки і завадозахищеності. При цьому як дискретні послідовності (ДП), які розширюють спектр (маніпулюють несучою частотою), повинні бути використані ДП, які засновані на нелінійних правилах побудови і мають покращені кореляційні, ансамблеві і структурні властивості. Запропоновано методи синтезу і формування нелінійних дискретних складних сигналів, а саме – так званих криптографічних сигналів. Перший метод, що представлено, використовує випадкові (псевдовипадкові) процеси. Інший метод засновано на реалізації операції децимації вихідної дискретної послідовності символів, яка отримана за результатами реалізації першого методу, і забезпечує синтез сис-

теми сигналів для визначеної тривалості сигналу. Отримані аналітичні вирази для визначення часу синтезу системи сигналів із застосуванням запропонованих методів. Показано, що швидкодія методу формування сигналів на основі операції децимації для визначеної тривалості сигналу більш ніж на три порядки перевищує швидкодію методу, що заснований на використанні випадкових (псевдовипадкових) процесів. На основі проведеного комп'ютерного моделювання показано, що сигнали, які отримані із застосуванням запропонованих методів, мають ідентичні властивості (кореляційні, ансамблеві, структурні).

*Ключові слова:* функція кореляції; дискретні послідовності; синтез систем сигналів; шумоподібний сигнал, стійкість перед перешкодами прийому сигналів; криптографічний сигнал; статистичні характеристики кореляційної функції, децимація.

Табл. 4. Бібліогр.: 10 назв.

УДК 621.391

**Методы синтеза и формирование системы нелинейных дискретных сигналов для современных информационно-коммуникационных систем** / *И.Д. Горбенко, А.А. Замула, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 126 – 132.

Приводятся результаты решения актуальной проблемы улучшения показателей эффективности функционирования информационно-коммуникационных систем (ИКС), в частности информационной безопасности, помехоустойчивости, скрытности, скорости формирования и обработки информации. Используемые методы формирования и обработки данных, а также классы широкополосных сигналов, применяемых в качестве физических переносчиков данных, не позволяют обеспечить необходимые (особенно для объектов критической инфраструктуры) показатели информационной безопасности и помехозащищенности. При этом в качестве дискретных последовательностей (ДП), которые расширяют спектр (манипулируют несущей частотой), должны быть использованы ДП, основанные на нелинейных правилах построения и имеющие улучшенные корреляционные, ансамблевые и структурные свойства.

Предложены методы синтеза и формирования нелинейных дискретных сложных сигналов, а именно так называемых криптографических сигналов. Первый метод, который представлен в статье, использует случайные (псевдослучайные) процессы. Другой метод основан на реализации операции децимации исходной дискретной последовательности символов, полученной по результатам реализации первого метода, и обеспечивает синтез ансамбля сигналов для определенной длительности сигнала.

Получены аналитические выражения для определения времени синтеза ансамбля сигналов с применением предложенных методов. Показано, что быстродействие метода формирования сигналов на основе операции децимации, для определенной длительности сигнала, более чем на три порядка превышает быстродействие метода, основанного на использовании случайных (псевдослучайных) процессов. На основе проведенного компьютерного моделирования показано, что сигналы, полученные с применением предложенных методов, обладают идентичными корреляционными, ансамблевыми, структурными свойствами.

*Ключевые слова:* функция корреляции; дискретные последовательности; синтез систем сигналов; шумоподобный сигнал, помехоустойчивость приема сигналов; криптографический сигнал; статистические характеристики корреляционной функции, децимация.

Табл. 4. Библиогр.: 10 назв.

UDC 621.391

**Methods of synthesis and formation of a system of nonlinear discrete signals for modern information and communication systems** / *I.D. Gorbenko, A.A. Zamula, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 126 – 132.

The paper presents the results of solving the urgent problem of improving the performance indicators of information and communication systems (ICS), in particular, information security, noise immunity, secrecy, the speed of formation and processing of information. The use of the distributed spectrum technology (broadband noise-like signals) is a promising direction for ensuring the security of information resources. The methods used for data formation and processing, as well as the classes of broadband signals used as physical data carriers, do not allow providing the necessary (especially for critical infrastructure facilities) indicators of information security and noise immunity. In this case, as discrete sequences (DS) that expand the spectrum (manipulate the carrier frequency), should be used DS based on nonlinear construction rules and having improved correlation, ensemble and structural properties. Methods for the synthesis and formation of nonlinear discrete complex signals, namely, the so-called cryptographic signals, are proposed. The first method, presented in the article, uses random (pseudo-random) processes. Another method is based on the implementation of the operation of decimation of the original discrete sequence of symbols obtained from the results of the implementation of the first method; it provides the synthesis of an ensemble of signals for a certain signal duration. Analytical expressions are obtained for determining the synthesis time of an ensemble of signals using the proposed methods. It is shown that the speed of the signal generation method based on the decimation operation for a certain signal duration is more than three orders of magnitude higher than the speed of the method based on the random (pseudo-random) processes used. At the same time, based on the carried out computer simulation, it is shown that the signals obtained using the proposed methods have identical correlation, ensemble, and structural properties.

*Key words:* correlation function; discrete sequences; synthesis of signal systems; noise-like signal, noise immunity of signal reception; cryptographic signal; statistical characteristics of the correlation function, decimation.

4 tab. Ref: 10 items.

УДК 621.391

**Порівняльний аналіз завадостійкості прийому нелінійних складних дискретних сигналів зі стандартними сигналами АФМ-16 BPSK /** *С.Г. Рассомахін, О.А. Замула, І.Д. Горбенко, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 133 – 140.

Показано, що рішення проблеми підвищення завадозахищеності (завадостійкості і скритності функціонування) ІКС може бути досягнуто на основі застосування систем нелінійних сигналів з поліпшеними ансамблевими, структурними і кореляційними властивостями. Розглянуто два класи нелінійних складних дискретних сигналів: характеристичні дискретні сигнали (ХДС) і криптографічні сигнали (КС). Представлено методи синтезу зазначених сигналів. Наведено статистична імітаційна модель для дослідження завадостійкості різних класів сигналів в гауссовому каналі. Із застосуванням такої моделі отримано оцінки ймовірності помилки у залежності від відношення сигнал/шум для різних класів сигналів, а саме ХДС, КС та стандартних сигналів BPSK АФМ-16. Показано, що для відношення сигнал/шум – 10, ймовірність помилки для ХДС складає 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким чином, використання нелінійних складних дискретних сигналів, зокрема ХДС та КС, дозволяє суттєво підвищити завадостійкість прийому сигналів у сучасних ІКС. Зважаючи на покращені ансамблеві і структурні властивості зазначених нелінійних сигналів, є можливість значно поліпшити показники крипто- і імітозахищеності функціонування систем.

*Ключові слова:* завадостійкість прийому; скритність; інформаційна безпека; дискретні послідовності; гаусів канал; ймовірність помилки; шумоподібний сигнал.

Табл. 1. Іл. 5. Бібліогр.: 10 назв.

УДК 621.391

**Сравнительный анализ помехоустойчивости приема нелинейных сложных дискретных сигналов со стандартными сигналами АФМ-16 BPSK** / *С.Г. Рассомахин, А.А. Замула, И.Д. Горбенко, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 133 – 140.

Показано, что решение проблемы повышения помехозащищенности (помехоустойчивости и скрытности функционирования) ИКС может быть достигнуто на основе применения систем нелинейных сигналов с улучшенными ансамблевыми, структурными и корреляционными свойствами. Рассмотрены два класса нелинейных сложных дискретных сигналов: характеристические дискретные сигналы (ХДС) и криптографические сигналы (КС). Представлены методы синтеза указанных сигналов. Приведена статистическая имитационная модель для исследования помехоустойчивости различных классов сигналов в гауссовом канале. С применением такой модели получены оценки зависимости вероятности ошибки от отношения сигнал / шум для различных классов сигналов, а именно: ХДС, КС и стандартных сигналов BPSK АФМ-16. Показано, что для отношения сигнал / шум – 10 вероятность ошибки для ХДС составляет 4.6875e-06, для КС – 3.515625e-06, а для – АФМ-16 – 0.002025. Таким образом, использование нелинейных сложных дискретных сигналов, в частности ХДС и КС, позволяет существенно повысить помехоустойчивость приема сигналов в современных ИКС. Учитывая улучшенные ансамблевые и структурные свойства указанных нелинейных сигналов, есть возможность значительно улучшить показатели крипто- и имитозащищенности функционирования систем.

*Ключевые слова:* помехоустойчивость приема; скрытность; информационная безопасность; дискретные последовательности; гауссов канал; вероятность ошибки; шумоподобный сигнал.

Табл. 1. Ил. 5. Библиогр.: 10 назв.

UDC 621.391

**Comparative analysis of noise immunity of reception of nonlinear complex discrete signals with standard signals AFM-16 BPSK /** *S.G. Rassomakhin, A.A. Zamula, I.D. Gorbenko, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 133 – 140.

The article shows that the solution to the problem of increasing the noise immunity (noise immunity and secrecy of functioning) of the ICS can be achieved using systems of nonlinear signals with improved ensemble, structural and correlation properties. Two classes of nonlinear complex discrete signals are considered: characteristic discrete signals (CDS) and cryptographic signals (CS). Methods for the synthesis of these signals are presented. The paper gives a statistical simulation model for studying the noise immunity of various classes of signals in the Gaussian channel. Using this model, estimates of the dependence of the error probability on the signal-to-noise ratio were obtained for various classes of signals, namely: CDS, KS and standard BPSK AFM-16 signals. It is shown that for the signal-to-noise ratio – 10 the error probability for the CDR is 4.6875e-06, for the CS is 3.515625e-06, and for the AFM-16 is 0.002025. Thus, the use of nonlinear complex discrete signals, in particular, CDS and KS, can significantly increase the noise immunity of signal reception in modern ICS. At the same time, taking into account the improved ensemble and structural properties of these nonlinear signals, it is possible to improve significantly the indicators of crypto- and imitation security of the systems functioning.

*Key words:* reception immunity; secrecy; information security; discrete sequences; Gaussian channel; error probability; noise-like signal.

1 tab. 5 fig. Ref: 10 items.

УДК 621.391

**Статистичні властивості похідних систем сигналів** / *О.А. Замула, І.Д. Горбенко, Хо Чі Лик* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 141 – 147.

Актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій і володіють необхідними кореляційними, структурними, ансамблевими властивостями. Авторами запропоновано метод синтезу похідних систем сигналів, для яких у якості вихідних застосовуються ортогональні сигнали, а у якості таких, що продукують, – нелінійні дискретні складні криптографічні сигнали (КС). Синтез останніх засновано на використанні випадкових (псевдовипадкових) процесів, у тому числі, алгоритмів криптографічного перетворення інформації. Синтезовані таким чином похідні сигнали володіють покращеними (у порівнянні з лінійними класами сигналів) ансамблевими і кореляційними властивостями, тоді як статистичні властивості таких систем сигналів є не вивченими. Наведено результати тестування похідних систем сигналів із застосуванням тестів, що визначені у FIPS PUB 140 та NIST 800-22. Аналіз результатів дозволяє стверджувати, що статистичні властивості даного класу похідних сигналів задовольняють вимогам, що пред'являються до псевдовипадкових послідовностей: непередбачуваність, незворотність, випадковість, незалежність символів і ін. По суті такі сигнали не відрізняються від випадкових послідовностей. Застосування запропонованого класу похідних сигналів дозволить поліпшити показники завадостійкості прийому сигналів, інформаційної безпеки і скритності функціонування ІКС.

*Ключові слова:* тестування похідних сигналів; дискретні послідовності; завадостійкість прийому сигналів; криптографічний сигнал; похідний сигнал; ортогональний сигнал; статистичні властивості сигналів.

Табл. 8. Бібліогр.: 10 назв.

УДК 621.391

**Статистические свойства производных систем сигналов** / *А.А. Замула, И.Д. Горбенко, Хо Чи Лык* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 141 – 147.

Актуальной проблемой остается поиск эффективных методов синтеза дискретных сигналов (последовательностей), соответствующих потенциально возможным предельным характеристикам корреляционных функций и обладающих необходимыми корреляционными, структурными, ансамблевыми свойствами. Авторами предложен метод синтеза производных систем сигналов, для которых в качестве исходных применяются ортогональные сигналы, а в качестве производящих – нелинейные дискретные сложные криптографические сигналы (КС). Синтез последних основан на использовании случайных (псевдослучайных) процессов, в том числе алгоритмов криптографического преобразования информации. Синтезированные таким образом производные сигналы обладают улучшенными (по сравнению с линейными классами сигналов) ансамблевыми и корреляционными свойствами, тогда как статистические свойства таких систем сигналов остаются не изученными. Приведены результаты тестирования производных систем сигналов с применением тестов, которые определены в FIPS PUB 140 и NIST 800-22. Анализ результатов позволяет утверждать, что статистические свойства данного класса производных сигналов удовлетворяют требованиям, предъявляемым к псевдослучайным последовательностям: непредсказуемость, необратимость, случайность, независимость символов и др. По сути, такие сигналы не отличаются от случайных последовательностей. Применение предложенного класса производных сигналов позволит улучшить показатели помехоустойчивости приема сигналов, информационной безопасности и скрытности функционирования ИКС.

*Ключевые слова:* тестирование производных сигналов; дискретные последовательности; помехоустойчивость приема сигналов; криптографический сигнал; производный сигнал; ортогональный сигнал; статистические свойства сигналов.

Табл. 8. Библиогр.: 10 назв.

UDC 621.391

**Statistical properties of derived signal systems** / *A.A. Zamula, I.D. Gorbenko, Ho Tri Luc* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 141 – 147.

The search for effective methods of synthesis of discrete signals (sequences) that correspond to the potentially possible limiting characteristics of correlation functions and possess the necessary correlation, structural, ensemble properties remains an urgent problem. The authors have proposed a method for the synthesis of derivatives of signal systems, for which orthogonal signals are used as the initial ones, and nonlinear discrete complex cryptographic signals (CS) are used as generating signals. The synthesis of the latter ones is based on the use of random (pseudo-random) processes, including algorithms for cryptographic information transformation. Derivative signals synthesized in this way have improved (in comparison with linear signal classes) ensemble and correlation properties, while the statistical properties of such signal systems remain unexplored. The paper presents the results of testing derived signal systems using the tests defined in FIPS PUB 140 and NIST 800-22. Analysis of the results obtained allows us to assert that the statistical properties of this class of derived signals satisfy the requirements for pseudo-random sequences: unpredictability, irreversibility, randomness, independence of symbols, etc. In essence, such signals do not differ from random sequences. The use of the proposed class of derived signals will improve the performance of signal reception noise immunity, information security and secrecy of the ICS functioning.

*Key words:* testing of derived signals; discrete sequences; noise immunity of signal reception; cryptographic signal; derived signal; orthogonal signal; statistical properties of signals.

8 tab. Ref: 10 items.

# РАДІОТЕХНІЧНІ СИСТЕМИ
# РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ
# RADIO ENGINEERING SYSTEMS

УДК 621.396.96, 621.397.48:004.932.2

**Комплексна обробка сигналів інтегрованої системи спостереження безпілотних літальних апаратів з використанням цілевказівки /** *В.М. Карташов, В.Н. Олейніков, В.І. Леонідов, В.В. Воронін, А.І. Капуста, І.С. Селєзнев, Є.В. Першин* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 148 – 161.

Одна з актуальних науково-технічних проблем сучасності полягає в розробці методів і засобів захисту різноманітних об'єктів від впливу безпілотних літальних апаратів (БПЛА), які становлять значну потенційну загрозу для різних областей діяльності людини – військової, господарської та повсякденної. Значні технічні можливості, широка номенклатура і порівняно невисока вартість БПЛА в поєднанні з труднощами їх спостереження і контролю – основні особливості даної проблеми. У даний час для виявлення і спостереження безпілотних літальних апаратів широко використовуються радіолокаційний, акустичний, оптичний і інфрачервоний методи і відповідні засоби.

У статті розглянуто інформаційні можливості кожного з методів і засобів, що входять до складу комплексної системи виявлення, вимірювання координат і параметрів руху БПЛА. Показано, що найкращими пошуковими можливостями володіє радіолокаційний метод, йому поступаються оптичний, інфрачервоний і акустичний методи. Обговорюється алгоритм послідовного підключення наявних в комплексній системі інформаційних ресурсів з урахуванням наявності у відповідних засобів пошукових можливостей.

Синтезовані нові ефективні методи комплексної обробки багатомодальних сигналів і зображень в інтегрованій комплексній системі спостереження безпілотних літальних апаратів, побудовані з урахуванням природного просторового ешелонування різних інформаційних каналів і з використанням цілевказівки. Показано особливості об'єднання багатомодальної інформації з використанням нейромережевих технологій при використанні цілевказань у комплексній системі.

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

Табл. 1. Іл. 5. Бібліогр.: 44 назв.

УДК 621.396.96, 621.397.48:004.932.2

**Комплексная обработка сигналов интегрированной системы наблюдения беспилотных летательных аппаратов с использованием целеуказания /** *В.М. Карташов, В.Н. Олейников, В.И. Леонидов, В.В. Воронин, А.И. Капуста, И.С. Селезнев, Е.В. Першин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 148 – 161.

Одна из актуальных научно-технических проблем современности заключается в разработке методов и средств защиты разнообразных объектов от воздействия беспилотных летательных аппаратов (БПЛА), несущих значительную потенциальную угрозу для различных областей деятельности человека – военной, хозяйственной и повседневной. Значительные технические возможности, широкая номенклатура и сравнительно невысокая стоимость БПЛА в сочетании с трудностями их наблюдения и контроля – основные особенности данной проблемы. В настоящее время для обнаружения и наблюдения беспилотных летательных аппаратов широко используются радиолокационный, акустический, оптический и инфракрасный методы и соответствующие средства.

Рассмотрены информационные возможности каждого из методов и средств, входящих в состав комплексной системы обнаружения, измерения координат и параметров движения БПЛА. Показано, что наилучшими поисковыми возможностями обладает радиолокационный метод, ему уступают оптический, инфракрасный и акустический методы. Обсуждается алгоритм последовательного подключения имеющихся в комплексной системе информационных ресурсов с учетом наличия у соответствующих средств поисковых возможностей.

Синтезированы новые эффективные методы комплексной обработки многомодальных сигналов и изображений в интегрированной комплексной системе наблюдения беспилотных летательных аппаратов, построенные с учетом естественного пространственного эшелонирования различных информационных каналов и с использованием целеуказания. Показаны особенности объединения многомодальной информации с использованием нейросетевых технологий при использовании целеуказаний в комплексной системе.

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

Табл. 1. Ил. 5. Библиогр.: 44 назв.

UDC 621.396.96, 621.397.48:004.932.2

**Complex processing of signals of integrated unmanned aerial vehicles surveillance system with the use of target designation /** *V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, V.I. Leonidov, V.V. Voronin, A.I. Kapusta, I.S. Selezniov, I.V. Pershyn* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 148 – 161.

One of the urgent scientific and technical problems of our time is the development of methods and means of protecting various objects against the impact of unmanned aerial vehicles (UAVs) which carry a significant potential threat

to various areas of human activity – military, economic and everyday life. Significant technical capabilities, a wide range and relatively low cost of UAVs, combined with the difficulties of their observation and control, are the main features of this problem. Currently, radar, acoustic, optical and infrared methods with the appropriate facilities are widely used to detect and observe unmanned aerial vehicles.

The article discusses the information capabilities of each of the methods and tools that are a part of an integrated system for detecting, measuring coordinates and parameters of UAV motion. It is shown that the radar method has the best search capabilities, while optical, infrared and acoustic methods are inferior to it. An algorithm for sequential connection of information resources available in an integrated system is discussed, taking into account the availability of search capabilities of the relevant means.

New effective methods of complex processing of multimodal signals and images in a complex integrated surveillance system for unmanned aerial vehicles, built taking into account the natural spatial separation of various information channels and using target designation, have been synthesized. The features of combining multimodal information with the use of neural network technologies when using target designations in an integrated system are shown.

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

1 tab. 5 fig. Ref: 44 items.

УДК 621.396.96:004.045

**Оптимізація обробки даних в літакових відповідачах системи ідентифікації «свій-чужий» /** *І.В. Свид, І.І. Обод, Г.Е. Заволодько* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 162 – 169.

Синтезована оптимальна структура обробки даних літакового відповідача системи ідентифікації «свій-чужий», на основі критерію Неймана – Пірсона. Показано, що при синтезі та аналізі оптимальної структури обробки сигнальних даних у літакових відповідачах систем ідентифікації «свій-чужий» необхідно враховувати багатоканальність прийому сигналів запиту та обмеження відносної пропускної здатності літакового відповідача, яка зумовлена наявним принципом побудови системи як одноканальної системи масового обслуговування з відмовами. Запропоновані моделі дозволяють реалізувати структури обробки даних сигналів запиту для ситуацій міжканального злиття попередніх канальних рішень про виявлення сигналів запиту або імпульсних складових сигналів запиту. В запропонованій структурі оптимізація обробки даних здійснюється не тільки за часовими, але й за просторовими параметрами сигналів запиту, а також враховується відносна пропускна здатність літакового відповідача. Показано, що міжканальне злиття результатів виявлення складових імпульсів сигналів запиту більш переважне в порівнянні з існуючим алгоритмом злиття результатів виявлення сигналів запиту, так як дозволяє підвищити якість виявлення сигналів запиту та знизити залежність ймовірності виявлення сигналів запиту від відносної пропускної здатності літакового відповідача.

*Ключові слова:* система ідентифікації «свій-чужий»; управління повітряним рухом; повітряний об’єкт; літаковий відповідач; обробка даних; сигнал запиту; сигнал відповіді; оптимізація; критерій Неймана – Пірсона; відносна пропускна здатність; алгоритм злиття.

Іл. 4. Бібліогр.: 28 назв.

УДК 621.396.96:004.045

**Оптимизация обработки данных в самолетных ответчиках системы идентификации «свой-чужой» /** *И.В. Свид, И.И. Обод, А.Э. Заволодько* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 162 – 169.

Синтезирована оптимальная структура обработки данных самолетного ответчика системы идентификации «свой-чужой», на основе критерия Неймана-Пирсона. Также показано, что при синтезе и анализе оптимальной структуры обработки сигнальных данных в самолетных ответчиках систем идентификации «свой-чужой» необходимо учитывать многоканальность приема сигналов запроса и ограничения относительной пропускной способности самолетного ответчика, которая обусловлена имеющимся принципом построения системы как одноканальной системы массового обслуживания с отказами. Предложенные модели позволяют реализовать структуры обработки данных сигналов запроса для ситуаций межканального слияния предыдущих канальных решений об обнаружении сигналов запроса или импульсных составляющих сигналов запроса. В предложенной структуре оптимизация обработки данных осуществляется не только по времени, но и по пространственным параметрам сигналов запроса, а также учитывается относительная пропускная способность самолетного ответчика. Показано, что межканальные слияния результатов выявления составляющих импульсов запросных сигналов более предпочтительно по сравнению с существующим алгоритмом слияния результатов обнаружения запросных сигналов, так как позволяет повысить качество обнаружения запросных сигналов и снизить зависимость вероятности обнаружения запросных сигналов от относительной пропускной способности самолетного ответчика.

*Ключевые слова:* система идентификации «свой-чужой»; управления воздушным движением; воздушный объект; самолетный ответчик; обработка данных; сигнал запроса; сигнал ответа; оптимизация; критерий Неймана – Пирсона; относительная пропускная способность; алгоритм слияния.

Ил. 4. Библиогр.: 28 назв.

UDC 621.396.96:004.045

**Optimization of data processing in aircraft transponder of the "friend or foe" identification system** / *I.V. Svyd, I.I. Obod, G.E. Zavolodko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 162 – 169.

The paper synthesizes the optimal structure of data processing of the aircraft transponder of the “friend or foe” identification system based on the Neumann-Pearson criterion. It is also shown, that when synthesizing and analyzing the optimal structure of signal data processing in aircraft transponders of "friend or foe" identification systems, it is necessary to take into account the multichannel reception of request signals and limitations of relative throughput of the aircraft transponder, which is caused by the existing principle of constructing the system as single-channel queuing system with failures. The proposed models make it possible to implement the structures of data processing of request signals for situations of inter-channel merging of previous channel decisions on the detection of request signals or pulse components of the request signals. In the proposed structure, the optimization of data processing is carried out not only in time but also in the spatial parameters of the request signals, and also takes into account the relative bandwidth of the aircraft responder. It is shown that the inter channel merging of the results of detecting the component pulses of the query signals is more preferable compared to the existing algorithm of merging the results of detecting the query signals, as it improves the quality of query signal detection and reduces the dependence of query signal detection of relative response.

*Key words:* identification system "friend or foe"; air traffic control; air object; aircraft respondent; Data Processing; request signal; response signal; optimization; Neumann-Pearson criterion; relative bandwidth; fusion algorithm.

4 fig. Ref: 28 items.

## ЕЛЕКТРОДИНАМІКА, ОПТИКА, ТЕХНІКА, НВЧ
## ЭЛЕКТРОДИНАМИКА, ОПТИКА, ТЕХНИКА СВЧ
## ELECTRODYNAMICS, OPTICS, MICROWAVE TECHNOLOGY

УДК 537.862

**Способи регулювання зворотного зв'язку в лазерах терагерцового діапазону** / *М.І. Дзюбенко, В.А. Маслов, В.П. Радіонов, А.А. Фомін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 170 – 175.

Оптимальний коефіцієнт зворотного зв'язку в активному відкритому резонаторі є важливою умовою високої ефективності лазерної генерації. Для точного підбору оптимуму зв'язку і підтримки оптимуму на всіх режимах роботи лазера необхідна можливість плавного регулювання зв'язку. У лазерах терагерцового (ТГц) діапазону є ряд особливостей, які необхідно враховувати при виборі схем регулювання зворотного зв'язку. В роботі наведено огляд і порівняльний аналіз схем лазерних резонаторів (ТГц) діапазону з плавним регулюванням виведення випромінювання. Розглянуто, як давно відомі і широко використовувані, так і новітні схеми лазерних резонаторів. Плавне регулювання вдається реалізувати в резонаторах які утворені металевими дзеркалами повного внутрішнього відбиття і вивідними дзеркалами у вигляді металевих дзеркал з отворами або одновимірних металевих решіток. Проведено аналіз переваг і недоліків кожної з розглянутих оптичних схем лазерних резонаторів.

Показано, що наведені схеми резонаторів дають можливість регулювати і оптимізувати зворотний зв'язок в лазері в процесі його роботи. Всі вони не відрізняються високою складністю і можуть бути реалізовані шляхом переобладнання діючих лазерів. Вибирати конкретну схему слід відповідно до специфіки застосування лазера. Застосування резонаторів з плавним регулюванням зв'язку дозволяє досягати високої ефективності лазерів на всіх енергетичних режимах роботи.

*Ключові слова:* терагерцові лазери; відкриті резонатори; плавне регулювання зворотного зв'язку.

Іл. 4. Бібліогр.: 8 назв.

УДК 537.862

**Способы регулировки обратной связи в лазерах терагерцевого диапазона** / *М.И. Дзюбенко, .А. Маслов, В.П. Радионов, А.А. Фомин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 170 – 175.

Оптимальный коэффициент обратной связи в активном открытом резонаторе является важным условием высокой эффективности лазерной генерации. Для точного подбора оптимума связи и поддержания оптимума на всех режимах работы лазера требуется возможность плавной регулировки связи. В лазерах терагерцевого (ТГц) диапазона имеется ряд особенностей, которые необходимо учитывать при выборе схем регулировки обратной связи. В работе приведен обзор и сравнительный анализ схем лазерных резонаторов (ТГц) диапазона с плавной регулировкой вывода излучения. Рассмотрены как давно известные и широко используемые, так и новейшие схемы лазерных резонаторов. Плавную регулировку удается реализовать в резонаторах, образованных металлическими зеркалами полного внутреннего отражения и выводными зеркалами в виде металлических зеркал с отверстиями или одномерных металлических решеток. Проведен анализ преимуществ и недостатков каждой из рассмотренных оптических схем лазерных резонаторов.

Показано, что приведенные схемы резонаторов дают возможность регулировать и оптимизировать обратную связь в лазере в процессе его работы. Все они не отличаются высокой сложностью и могут быть реализованы путем переоборудования действующих лазеров. Выбирать конкретную схему следует в соответствии со спецификой применения лазера. Применение резонаторов с плавной регулировкой связи позволяет добиваться высокой эффективности лазеров на всех энергетических режимах работы.

*Ключевые слова:* терагерцевые лазеры; открытые резонаторы; плавная регулировка обратной связи.

Ил. 4. Библиогр.: 8 назв.

UDC 537.862

**Methods for adjusting feedback in terahertz lasers** / *M.I. Dzyubenko, V.A. Maslov, V.P. Radionov, A.A. Fomin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 170 – 175.

The optimal feedback coefficient in an active open resonator is an important condition for high lasing efficiency. For precise selection of the optimum communication and maintaining the optimum in all modes of laser operation, the ability to adjust smoothly the communication is required. Terahertz (THz) lasers have a number of features that one should take into account when choosing feedback control schemes. The paper presents a review and comparative analysis of the schemes of laser resonators (THz) in the range with a smoothly controlled radiation output. The authors consider both long known and widely used, as well as the latest schemes of laser resonators. Smooth adjustment can be realized in resonators formed by metal mirrors of total internal reflection and output mirrors in the form of metal mirrors with holes or one-dimensional metal gratings. The analysis of the advantages and disadvantages of each of the considered optical schemes of laser resonators is carried out.

It is shown that the given resonator schemes make it possible to control and optimize the feedback in the laser during its operation. All of them are not very complex and can be realized by re-equipping existing lasers. The choice of a specific scheme should be made in accordance with the specifics of the laser application. The use of resonators with smooth coupling control makes it possible to achieve high efficiency of lasers at all energy operating modes.

*Key words:* terahertz lasers; open resonators; smooth feedback control.

4 fig. Ref: 8 items.

УДК 537.226.3

**Однорезонаторний НВЧ пристрій для контролю комплексної диелектричної проникності рідких паливно-мастильних матеріалів** / *Б.В. Жуков, С.І. Борбульов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 176 – 180.

Представлена спрощена структурна схема однорезонаторного НВЧ діелектрометра, призначеного для контролю комплексної діелектричної проникності рідких паливно-мастильних матеріалів. Розглянуто структурну схему НВЧ датчика діелектрометра, виконаного у вигляді паралелепіпеда, всередині якого розміщені хвилеведучі тракти, резонатор, керований і опорний генератори, змішувальний і детекторні діоди і атенюатори. Наведено загальний вигляд нижньої частини корпусу НВЧ датчика.

Розглянуто методику початкового налаштування НВЧ датчика, в процесі якої встановлюється початкові частоти керованого і опорного генераторів і визначається діапазон електронної перебудови частоти керованого генератора.

Наведено методику калібрування діелектрометра по порожній кюветі, яка дозволяє визначити придатність кювети для її використання при проведенні вимірювання комплексної діелектричної проникності зразків паливно-мастильних матеріалів, а також виключити вплив розкиду діелектричної проникності матеріалу кювети на результати вимірювання комплексної діелектричної проникності зразків ПММ.

Розглянуто методику дослідження параметрів зразків паливно-мастильних матеріалів, на підставі вимірів якої дані вимірювань представляються на комплексній площині для виконання аналізу отриманих результатів.

Наведено методику дослідження відмінності зразка паливно-мастильних матеріалу від його еталона, яка включає вимірювання параметрів порожній кювети, вимір дійсної та уявної складових комплексної діелектричної проникності зразка паливно-мастильних матеріалу і його еталона та аналіз відмінностей їх дійсних і уявних складових на комплексній площині.

*Ключові слова:* діелектрометр; резонатор; пально-мастильні матеріали; комплексна площина; кювета; еталон; діелектрична проникність; надвисокочастотний датчик.

Іл. 4. Бібліогр.: 3 назв.

УДК 537.226.3

**Однорезонаторное СВЧ устройство для контроля комплексной диэлектрической проницаемости жидких горюче-смазочных материалов** / *Б.В. Жуков, С.И. Борбулев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 176 – 180.

Представлена упрощенная структурная схема однорезонаторного СВЧ диэлектрометра, предназначенного для контроля комплексной диэлектрической проницаемости жидких горюче-смазочных материалов. Рассмотрена структурная схема СВЧ датчика диэлектрометра, выполненного в виде параллелепипеда, внутри которого размещены волноведущие тракты, резонатор, управляемый и опорный генераторы, смесительный и детекторный диоды и аттенюаторы. Приведен общий вид нижней части корпуса СВЧ датчика.

Рассмотрена методика первоначальной настройки СВЧ датчика, в процессе которой выполняется установка начальных частот управляемого и опорного генераторов и определение диапазона электронной перестройки частоты управляемого генератора.

Приведена методика калибровки диэлектрометра по пустой кювете, которая позволяет определить пригодность кюветы для ее использования при проведении измерения комплексной диэлектрической проницаемости образцов горюче-смазочных материалов, а также исключить влияние разброса диэлектрической проницаемости материала кюветы на результаты измерения комплексной диэлектрической проницаемости образцов ГСМ.

Рассмотрена методика исследования параметров образцов горюче-смазочных материалов, на основании измерений которой данные измерений представляются на комплексной плоскости для выполнения анализа полученных результатов.

Приведена методика исследования отличия образца горюче-смазочного материала от его эталона, которая включает измерение параметров пустой кюветы, измерение действительной и мнимой составляющих комплексной диэлектрической проницаемости образца горюче-смазочного материала и его эталона и анализ отличий их действительных и мнимых составляющих на комплексной плоскости.

*Ключевые слова:* диэлектрометр; резонатор; горючесмазочные материалы; комплексная плоскость; кювета, эталон; диэлектрическая проницаемость; сверхвысокочастотный датчик.

Ил. 4. Библиогр.: 3 назв.

UDC 537.226.3

**Single resonator microwave device for monitoring the complex dielectric constant of liquid fuels and lubricants** / *B.V. Zhukov, S.I. Borbulev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 176 – 180.

A simplified structural diagram of a single-cavity microwave dielectric meter designed to control the complex permittivity of liquid fuels and lubricants is presented. The structural diagram of the microwave sensor of the dielectrometer, made in the form of a parallelepiped, inside which waveguide paths, a resonator, controlled and reference generators, mixing and detector diodes and attenuators is considered. A general view of the lower part of the microwave sensor housing is given.

The technique of initial tuning of the microwave sensor is considered, during which the initial frequencies of the controlled and reference oscillators are set and the range of electronic frequency tuning of the frequency of the controlled generator is determined.

A method for calibrating a dielectrometer with an empty cuvette is presented. This method makes it possible to determine the suitability of the cuvette for its use in measuring the complex dielectric constant of samples of fuels and lubricants, and to exclude the influence of the dispersion of the dielectric constant of the material of the cuvette on the results of measuring the complex dielectric constant of fuels and lubricants.

The technique of studying the parameters of samples of fuels and lubricants is considered, based on which the measurement data are presented on a complex plane for analyzing the results obtained.

A technique for studying the difference between a fuel and lubricant sample and its standard is presented, which includes measuring the parameters of an empty cell, measuring the real and imaginary components of the complex dielectric constant of the fuel and lubricant sample and its standard, and analyzing the differences between their real and imaginary components on a complex plane.

*Key words:* dielectric meter; resonator; fuels and lubricants; complex plane; cuvette; standard; dielectric constant; microwave sensor.

4 fig. Ref: 3 items.

УДК 537.86

**Розсіювання електромагнітних хвиль дискретним октаедром з резонансних сфер** / *А.І. Козар* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 181 – 185.

Наведено рішення задачі про розсіяння електромагнітних хвиль дискретним опуклим многогранником – октаедром з резонансних магнітодіелектричних сфер на основі складної ромбічної кристалічної решітки.

Тут розглядається випадок, еквівалентний рентгенівській оптики кристалів, коли $a/\lambda' << 1$ і може бути $a/\lambda_g \sim 1; d,h,l/\lambda' \sim 1$, де $a$ – радіус сфер; $\lambda', \lambda_g$ – довжини розсіяної хвилі поза і всередині сфер; $d,h,l$ – постійні решітки. Рішення задачі отримано на основі інтегральних рівнянь електродинаміки Фредгольма 2-го роду, з нелокальними граничними умовами.

Знайдені у роботі вирази для метакрістала у формі октаедра можна використати для вивчення розсіяних кристалом полів в зонах Френеля і Фраунгофера, а також для вивчення його внутрішнього поля.

Отримані в роботі співвідношення можуть знайти застосування при вивченні розсіювання хвиль різного роду опуклими многогранниками, створення на їх основі нових видів обмежених метакристалів, в тому числі і нанокристалів з резонансними властивостями і при вивченні їх поведінки в різних зовнішніх середовищах.

А також при розробці методів моделювання електромагнітних явищ, які можуть відбуватися в реальних кристалах в резонансних областях в оптичному і рентгенівському діапазонах довжин хвиль.

*Ключові слова:* електромагнітні хвилі; сфера; кристал; рівняння; октаедр.

Іл. 1. Бібліогр.: 5 назв.

УДК 537.86

**Рассеяние электромагнитных волн дискретным октаэдром из резонансных сфер** / *А.И. Козарь* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 181 – 185.

Приведено решение задачи о рассеянии электромагнитных волн дискретным выпуклым многогранником – октаэдром из резонансных магнитодиэлектрических сфер на основе сложной ромбической кристаллической решетки.

Здесь рассматривается случай, эквивалентный рентгеновской оптике кристаллов, когда $a/\lambda' << 1$ и может быть $a/\lambda_g$ ~1; $d,h,l/\lambda'$ ~1, где $a$ – радиус сфер; $\lambda', \lambda_g$ – длины рассеиваемой волны вне и внутри сфер; $d,h,l$ – постоянные решетки. Решение задачи получено на основе интегральных уравнений электродинамики Фредгольма 2-го рода с нелокальными граничными условиями.

Найденные в работе выражения для метакристалла в форме октаэдра можно использовать для изучения рассеянных кристаллом полей в зонах Френеля и Фраунгофера, а также для изучения его внутреннего поля.

Полученные в работе соотношения могут найти применение при изучении рассеяния волн различного рода выпуклыми многогранниками, создания на их основе новых видов ограниченных метакристаллов, в том числе и нанокристаллов с резонансными свойствами и при изучении их поведения в различных внешних средах. А также при разработке методов моделирования электромагнитных явлений, которые могут происходить в реальных кристаллах в резонансных областях в оптическом и рентгеновском диапазонах длин волн.

*Ключевые слова:* электромагнитные волны; сфера; кристалл; уравнение; октаэдр.

Ил. 1. Библиогр.: 5 назв.

UDC 537.86

**Scattering of electromagnetic waves by a discrete octahedron from resonant spheres** / *A.I. Kozar* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 00 – 00.

A solution is given to the problem of scattering of electromagnetic waves by a discrete convex polyhedron – an octahedron of resonant magnetodielectric spheres based on a complex rhombic crystal lattice.

Here we consider a case equivalent to the X-ray optics of crystals, when $a/\lambda' << 1$ and can be $a/\lambda_g$ ~1; $d,h,l/\lambda'$ ~1, where $a$ is the radius of the spheres; $\lambda', \lambda_g$ are the lengths of the scattered wave outside and inside the spheres; $d,h,l$ are constant lattices. The solution of the problem is obtained based on the Fredholm integral equations of electrodynamics of the second kind with nonlocal boundary conditions.

The expressions found in this work for a metacrystal in the form of an octahedron can be used to study the fields scattered by the crystal in the Fresnel and Fraunhofer zones, as well as to study its internal field.

The relations obtained in this work can find application in the study of the scattering of waves of various kinds by convex polyhedrons, the creation on their basis of new types of limited metacrystals, including nanocrystals with resonance properties, and in the study of their behavior in various external media. As well as in the development of methods for modeling electromagnetic phenomena that can occur in real crystals in resonance regions in the optical and X-ray wavelength ranges.

*Key words:* electromagnetic waves; sphere; crystal; equation; octahedron.

1 fig. Ref: 5 items.

## ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ
## ПРИМЕНЕНИЕ МЕТОДОВ РАДИОТЕХНИКИ
## APPLICATION OF METHODS OF RADIO ENGINEERING

УДК 615.472.03

**Дослідження частотних характеристик імпедансу біологічних тканин** / *В.В. Семенець, В.І. Леонідов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 186 – 190.

Формулюється постановка задачі виявлення інформативних ознак життєздатності біологічних тканин при використанні методу імпедансометрії. Показано, що оскільки в цей час у медичній діагностичній практиці відсутня приладова база, що дозволяє в оперативній обстановці здійснювати діагностику здатності біологічної тканини до самовідновлення після одержання травм і поразок у результаті термічного впливу, вогнепального поранення або тривалого здавлювання, то розробка методів і засобів інструментальної діагностики в цій галузі знань є важливим сучасним завданням.

Приводяться результати експериментальних вимірів характеристик імпедансу в діапазоні частот 20 Гц – 2,0 МГц. Аналізуються частотні залежності модуля напруги на біотканини рослинного походження при її неушкодженому стані, а також після витримки зразків біотканини в морозильній камері на інтервалах часу від 15 хв до двох годин.

Проводиться порівняльний аналіз отриманих частотних залежностей. Показано істотну відмінність частотних залежностей модуля напруги на біотканини від частотної залежності модуля напруги на ізотонічному розчині. Вводиться поняття про те, що критерієм оцінки ступеня поразки біотканини може служити ступінь відмінності частотного розподілу модуля імпедансу біотканини від модуля імпедансу ізотоничного розчину.

Формулюється висновок про доцільність розвитку методу імпедансометрії як методу діагностики життєздатності біотканини, показано, що найбільш перспективним підходом до розвитку методів імпедансометрії є аналіз перехідних процесів при збурюванні біотканини імпульсами електричного струму малої величини.

*Ключові слова:* імпедансометрія; життєздатність; частотна характеристика; інформативні ознаки.

Іл. 3. Бібліогр.: 15 назв.

УДК 615.472.03

**Исследование частотных характеристик импеданса биологических тканей** / *В.В. Семенец, В.И. Леонидов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 186 – 190.

Формулируется постановка задачи выявления информативных признаков жизнеспособности биологических тканей при использовании метода импедансометрии. Показано, что так как в настоящее время в медицинской диагностической практике отсутствует приборная база, позволяющая в оперативной обстановке осуществлять диагностику способности биологической ткани к самовосстановлению после получения травм и поражений в результате термического воздействия, огнестрельного ранения или длительного сдавливания, то разработка методов и средств инструментальной диагностики в этой области знаний является важной современной задачей.

Приводятся результаты экспериментальных измерений характеристик импеданса в диапазоне частот 20 Гц – 2,0 МГц. Анализируются частотные зависимости модуля напряжения на биоткани растительного происхождения при ее неповрежденном состоянии, а также после выдержки образцов биоткани в морозильной камере на интервалах времени от 15 мин до 2-х часов.

Проводится сопоставительный анализ полученных частотных зависимостей. Показано существенное отличие частотных зависимостей модуля напряжения на биоткани от частотной зависимости модуля напряжения на изотоническом растворе. Вводится понятие о том, что критерием оценки степени поражения биоткани может служить степень отличия частотного распределения модуля импеданса биоткани от модуля импеданса изотонического раствора.

Приводится вывод о целесообразности развития метода импедансометрии как метода диагностики жизнеспособности биоткани, показано, что наиболее перспективным подходом к развитию методов импедансометрии есть анализ переходных процессов при возмущении биоткани импульсами электрического тока малой величины.

*Ключевые слова:* импедансометрия; жизнеспособность; частотная характеристика; информативные признаки.

Ил. 3. Библиогр.: 15 назв.

UDC 615.472.03

**Investigation of frequency characteristics of biological tissues impedance** / *V.V. Semenetz, V.I. Leonidov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 186 – 190.

The problem of identifying informative signs of biological tissues viability using the impedance measurement method is formulated. At present there is no instrumental base that makes it possible in an operational setting to diagnose the ability of biological tissue to heal itself after injury and damage as a result of thermal exposure, gunshot wound or prolonged compression. It is shown in this article that development of methods and tools for instrumental diagnostics in medical diagnostic practice is an important modern challenge.

The results of experimental measurements of impedance characteristics in the frequency range of 20 Hz – 2.0 MHz are presented. The frequency dependences of the modulus of voltage on biological tissues of plant origin are analyzed in its intact state, as well as after exposure of biological tissue samples in a freezer at time intervals from 15 minutes to 2 hours.

A comparative analysis of the obtained frequency dependences is carried out. A significant difference between the frequency dependences of the voltage modulus on biological tissues and the frequency dependence of the voltage modulus on an isotonic solution is shown. The concept is introduced that the degree of difference between the frequency distribution of the biological tissue impedance module from the impedance module of an isotonic solution can serve as a criterion for assessing the degree of damage to biological tissue.

A conclusion is made about the advisability of developing the impedance measurement method as a method for diagnosing the viability of biological tissue; it is shown that the most promising approach to the development of impedance measurement methods is the analysis of transient processes when biological tissue is disturbed by small electric current pulses.

*Key words:* impedance measurement; viability; frequency response; informative signs.

3 fig. Ref: 15 items.

# ОБРОБКА СИГНАЛІВ
# ОБРАБОТКА СИГНАЛОВ
# SIGNAL PROCESSING

УДК 004.932

**Порівняльний аналіз алгоритмів суміщення зображень: нормована кореляція проти суміщення на основі SIFT /** *В.А. Душепа, Є.А. Тягнирядно, І.В. Баришев* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 191 – 196.

Проведено порівняння алгоритмів суміщення зображень: класичної нормованої кореляції (як представника алгоритмів, заснованих на інтенсивностях пікселів) і алгоритму, заснованого на SIFT (суміщення на основі ознак). Для нормованої кореляції також використовувався градієнтний алгоритм субпіксельної корекції. Було проведено порівняння ефективності їх роботи на реальних зображеннях (в тому числі карті місцевості) при моделюванні штучних спотворень. Досліджувалася точність визначення положення (зміщення) одного зображення щодо іншого при наявності повороту і зміни масштабу. Експеримент був проведений за допомогою імітаційної моделі, створеної мовою програмування Python при використанні бібліотеки комп'ютерного зору OpenCV.

Результати експериментів показують, що при відсутності повороту і зміни масштабу між зображеннями, що суміщуються, нормована кореляція забезпечує дещо меншу середньоквадратичну помилку. При цьому за наявності навіть невеликих таких спотворень, наприклад, повороту більш ніж на два градуси і зміни масштабу більш ніж на два відсотки, вірогідність правильного суміщення для нормованої кореляції різко падає. Також було відзначено, що перевагами нормованої кореляції є майже в п’ять разів більша швидкодія і можливість її використання для невеликих фрагментів (50x50 і менше), де для алгоритму SIFT проблематично виділити достатню кількість ключових точок.

Також показано, що використання двоетапного алгоритму (суміщення на основі SIFT на першому етапі, і оптимізація з нормованою кореляцією у якості критерію на другому) дозволяє отримати одночасно і високу точність, і стійкість до повороту і зміни масштабу, ціною великих обчислювальних витрат.

*Ключові слова:* алгоритми суміщення зображень; нормована кореляція; SIFT; python; OpenCV.

Іл. 7. Бібліогр.: 15 назв.

УДК 004.932

**Сравнительный анализ алгоритмов совмещения изображений: нормированная корреляция против совмещения на основе SIFT /** *В.А. Душепа, Е.А. Тягнырядно, И.В. Барышев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 191 – 196.

Проведено сравнение алгоритмов совмещения изображений: классической нормированной корреляции (как представителя алгоритмов, основанных на интенсивностях пикселей) и алгоритма, основанного на SIFT (совмещение на основе признаков). Для нормированной корреляции также использовался градиентный алгоритм субпиксельной коррекции. Было проведено сравнение эффективности их работы на реальных изображениях (в том числе карте местности) при моделировании искусственных искажений. Исследовалась точность определения положения (смещения) одного изображения относительно другого при наличии поворота и изменения масштаба. Эксперимент был проведен с помощью имитационной модели, созданной на языке программирования Python при использовании библиотеки компьютерного зрения OpenCV.

Результаты экспериментов показывают, что при отсутствии поворота и изменения масштаба между совмещаемыми изображениями нормированная корреляция обеспечивает несколько меньшую среднеквадратическую ошибку. При этом при наличии даже небольших таких искажений, например поворота более чем на два градуса и изменения масштаба более чем на два процента, вероятность правильного совмещения для нормированной корреляции резко падает. Также было отмечено, что преимуществами нормированной корреляции является почти в пять раз большее быстродействие и возможность ее использования для небольших фрагментов (50x50 и менее), где для алгоритма SIFT проблематично выделить достаточное количество ключевых точек.

Также показано, что использование двухэтапного алгоритма (совмещение на основе SIFT на первом этапе, и оптимизация с нормированной корреляцией в качестве критерия на втором) позволяет получить одновременно и высокую точность, и устойчивость к повороту и изменению масштаба, ценой больших вычислительных затрат.

*Ключевые слова:* алгоритмы совмещения изображений; нормированная корреляция; SIFT; python; OpenCV.

Ил. 7. Библиогр.: 15 назв.

UDC 004.932

**Comparative analysis of algorithms for images fusion: normalized correlation versus fusion based on SIFT** / *V.A. Dushepa, Y.A. Tiahnyriadno, I.V. Baryshev* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 191 – 196.

The paper compares the image registration algorithms: the classical normalized correlation (as a representative of intensity-based algorithms) and the SIFT-based algorithm (feature-based registration). A gradient subpixel correction algorithm was also used for normalized correlation. We compared the effectiveness of their work on real images (in-

cluding a terrain map) when modeling artificial distortions. The accuracy of determining the position (shift) of one image relative to another in the presence of rotation and scale changes was studied. The experiment was carried out using a simulation model created in the Python programming language using the OpenCV computer vision library.

The results of the experiments show that in the absence of rotation and scale changes between the registered images the normalized correlation provides a slightly smaller root-mean-square error. At the same time, if there are even small such distortions, for example, a rotation of more than 2 degrees and a scale change of more than 2 percent, the probability of correct registration for the normalized correlation drops sharply. It was also noted that the advantages of normalized correlation are almost 5 times higher speed and the possibility of using it for small fragments (50x50 or less), where it is problematic for the SIFT algorithm to allocate a sufficient number of keypoints.

It was also shown that the use of a two-stage algorithm (SIFT-based registration at the first stage, and optimization with normalized correlation as a criterion at the second) allows you to get both high accuracy and stability to rotation and scale change, but this will be accompanied by high computational costs.

*Key words:* image registration algorithms; normalized correlation; SIFT; python; OpenCV.

7 fig. Ref: 15 items.

УДК 004.89: 621.396

**Семантичний аналіз флуктуацій радіолокаційної пачки для ідентифікації повітряних об'єктів** / *В.В. Жирнов, С.В. Солонська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 203. С. 197 – 203.

Розроблено та програмно реалізовано метод семантичного аналізу амплітудних флуктуацій радіолокаційної пачки для ідентифікації повітряних об'єктів в оглядових РЛС. Метод заснований на визначенні семантичних складових на етапі формування й аналізу символьної моделі пачки імпульсних сигналів від рухомих повітряних об'єктів. Сигнальна інформація описується предикатною функцією процесних знань формування та аналізу символьної моделі пачки імпульсних сигналів від рухомих повітряних об'єктів типу літак, вертоліт, БПЛА, та від атмосферних неоднорідностей типу «ангел-луна». В результаті семантичного аналізу амплітудних флуктуацій пачки в тимчасовій області отримані класифікаційні відмітні ознаки флуктуацій пачки від віддзеркалень, що заважають, і повітряних об'єктів. Досліджено семантичні складові алгоритму прийняття рішень, які подібні алгоритмам прийняття рішень оператором. У розробленому алгоритмі сигнальна інформація описується предикатною функцією на множині амплітуд імпульсів пачки, які перевищили певне порогове значення. Ідентифікація типів флуктуацій проводиться шляхом вирішення розроблених рівнянь предикатних операцій. На підставі отриманих рівнянь синтезована функціональна схема автоматичного визначення типів флуктуацій. Верифікація розробленого методу проведена на реальних даних, отриманих на оглядовій РЛС сантиметрового діапазону (тривалість імпульсу 1 мкс, частота зондування 365 Гц, період огляду 10 с). На основі цих даних змодельовані типи характерних пачок радіолокаційних сигналів. За результатами експериментів все вони були правильно ідентифіковані.

*Ключові слова:* семантичний аналіз; радіолокаційний сигнал; ідентифікація; заважаючи відбиття; повітряний об'єкт.

Іл. 3. Бібліогр.: 12 назв.

УДК 004.89: 621.396

**Семантический анализ флуктуаций радиолокационной пачки для идентификации воздушных объектов** / *В.В. Жирнов, С.В. Солонская* // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2020. Вып. 203. С. 197 – 203.

Разработан и программно реализован метод семантического анализа амплитудных флуктуаций радиолокационной пачки для идентификации воздушных объектов в обзорных РЛС. Метод основан на определении семантических составляющих на этапе формирования и анализа символьной модели пачки импульсных сигналов от подвижных воздушных объектов. Сигнальная информация описывается предикатной функцией процессных знаний формирования и анализа символьной модели пачки импульсных сигналов от подвижных летательных аппаратов типа самолет, вертолет, БПЛА, и от атмосферных неоднородностей типа «ангел-эхо. В результате семантического анализа амплитудных флуктуаций пачки во временной области получены классификационные отличительные признаки флуктуаций пачки от мешающих отражений и воздушных объектов. Исследованы семантические составляющие алгоритма принятия решений, которые подобны алгоритмам принятия решений оператором. В разработанном алгоритме сигнальная информация описывается предикатной функцией на множестве амплитуд импульсов пачки, превысивших некоторое пороговое значение. Идентификация типов флуктуаций проводится путем решения разработанных уравнений предикатных операций. На основании полученных уравнений синтезирована функциональная схема автоматического определения типов флуктуаций. Верификация разработанного метода проведена на реальных данных, полученных на обзорной РЛС сантиметрового диапазона (длительность импульса 1 мкс, частота зондирования 365 Гц, период обзора 10 с). На основе этих данных смоделированы типы характерных пачек радиолокационных сигналов. По результатам экспериментов все они были правильно идентифицированы.

*Ключевые слова:* семантический анализ; радиолокационный сигнал; идентификация; мешающие отражения; воздушный объект.

Ил. 3. Библиогр.: 12 назв.

UDC 004.89: 621.396

**Semantic analysis of fluctuations of a radar pack for identification of air objects** / *V. Zhyrnov, S. Solonskaya* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2020. №203. P. 197 – 203.

A method for semantic analysis of amplitude fluctuations of the radar pack to identify air objects in surveillance radars has been developed and implemented in software. This method is based on the determination of semantic components at the stage of formation and analysis of the symbolic model of a burst of impulse signals from mobile aircraft. Signal information is described by the predicate function of the process knowledge of the formation and analysis of the symbolic model of a burst of impulse signals from mobile aircraft such as an airplane, helicopter, UAV, and from atmospheric inhomogeneities of the angel-echo type. As a result of semantic analysis of the amplitude fluctuations, classification distinguishing attributes of fluctuations from interfering reflections and air objects are obtained. The semantic components of the decision-making algorithm, which are similar to decision-making algorithms by the operator, are investigated. In the developed algorithm, the signal information is described by a predicate function on the set of amplitudes of burst pulses exceeding a certain threshold value. Identification of the types of fluctuations is carried out by solving the developed equations of predicate operations. Based on these equations, a functional diagram of automatic determination of the fluctuation types is synthesized. The verification of the developed method was carried out on real data obtained on a survey centimeter-band radar (pulse duration 1 μs, sounding frequency 365 Hz, survey period 10 s). Based on these data, types of characteristic packs of radar signals are simulated. According to the results of the experiments, they were all correctly identified.

*Key words:* semantic analysis; radar signal; identification; interfering reflections; air object.

3 fig. Ref: 12 items.