МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

РАДИОТЕХНИКА

Всеукраинский межведомственный научно-технический сборник

ТЕМАТИЧЕСКИЙ ВЫПУСК
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Основан в 1965 г.

В Ы П У С К 1 9 1

Харків
Харківський національний
університет радіоелектроніки
2017

УДК 621.3

Сборник включен в список специальных изданий ВАК Украины по физико-математическим и техническим наукам.
Регистрационное свидетельство КВ № 12098-969 ПР от 14. 12. 2006.
Ответственность за содержание статей несут авторы.

Ответственные за выпуск: И.Д. Горбенко, д-р техн. наук, проф, А.И. Лучанинов, д-р физ.-мат. наук, проф.
Технический секретарь Е.С. Полякова

Рекомендовано Ученым советом Харьковского национального университета радиоэлектроники, протокол № 60 от 22.12.2017.

Адрес редакционной коллегии: Харьковский национальный университет радиоэлектроники (ХНУРЭ), просп. Науки, 14, Харьков, 61166, тел. (0572) 7021-397.

Сборник «Радиотехника» включен в Каталог подписных изданий Украины, подписной индекс ***08391***

СОДЕРЖАНИЕ

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

CONTENT

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

SYSTEMS OF INFORMATION PROCESSING AND PROTECTION

RADIO ENGINEERING AND TELECOMMUNICATIONS NETWORKS AND SYSTEMS

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

UDC 004.056.55

O. KACHKO, Yu. GORBENKO, M. YESINA, O. AKOLZINA

ASYMMETRIC ENCRYPTION ALGORITHM OPTIMIZATION BASED ON USING NTRU PRIME MATHEMATICS

Introduction

The development in quantum computer creation caused the need to search for quantum-resistant cryptographic algorithms and requirements formation for them. So NIST at the fall of 2017 announced a request for post-quantum algorithms search, including algorithms for asymmetric encryption [2]. It is known, for practical application, algorithms have to satisfy the requirements of resistance, performance and should be lightweight. During the work, optimization of a perspective post-quantum encryption NTRU-like algorithm was carried out. The encryption scheme from standard ANSI X9.98-2010 [1] and NTRU Prime parameters [3] were used in implementation.

1. NTRU Prime cryptosystem

Parameters for key generation, encryption and decryption, their appointment and formulas are specified in table 1 below. Then we describe formulas for keys generation, encryption and decryption according to [3].

Table 1

Denotation	Appointment	Formula
n	Polynomial order. Determines the number of its coefficients. A prime number for which the polynomial $x^n - x - 1$ is irreducible.	$n \geq \max\{3, 2t\}$
R	Field of polynomials $Z[x]$ with modulus $x^n - x - 1$.	$Z[x]/(x^n - x - 1)$
$R/3$	Field of polynomials $(Z/q)[x]$ with modulus $x^n - x - 1$.	$(Z/3)[x]/(x^n - x - 1)$
R/q	Field of polynomials $(Z/q)[x]$ with modulus $x^n - x - 1$.	$(Z/q)[x]/(x^n - x - 1)$
p	Smaller modulus.	$p = 3$
q	Bigger modulus, a prime number, by which all coefficients of a polynomial R/q are reduced.	$q \geq 48t + 3$
t	The natural number, determines the number of non-zero elements of a polynomial.	$t \geq 1$
k	Security strength (level).	
m	Secret message. The number of 0, 1 and -1, is bigger or equal t.	$m \in R/3$
e	Encrypted message.	$e \in R/q$
g	Random polynomial, that has $2N/3$ non-zero elements. The number of 1 and -1 is not necessarily equal. The secret parameter used to calculate the public key.	$g \in R/3$
f	Random t-small element (polynomial) is a secret.	$f = (1 + 3F) \bmod q$ $f \in R/q$
F	Random t-small element (polynomial) that defines a private key	$F \in R/3$
h	The sender's public key. Invertible element in R/q. The length of h is equal to $n\lceil \log_2 q \rceil$.	$h = 3g/f \in R/q$
r	Blinding polynomial, random t-small element.	$r \in R/3$
b	Random sequence (salt) that pads the message (Length of b is defined by security strength).	

Keys generation. By definition secret key is a polynomial f, $f = (1+3F) \bmod q$, where $F \in R/3$, the number of non-zero elements $\| F \|_1 = 2t$, and corresponding public key is polynomial $h = 3g / f \in R/q$, where $g \in R/3$.

For any secret key f and corresponding public key h define *encryption* and *decryption* functions E_h and D_f:

$$e = E_h(m,r) = (m + rh) \bmod q,\ m,r \in R/3,\ \| r \|_1 = 2t, \quad (1)$$

$$D_f(e) = (ef \,(\bmod q) \bmod 3,\ e \in R/q. \quad (2)$$

2. Experimental research of multiplying algorithms

Encryption and decryption algorithms use the multiplication functions of polynomials that have big computational complexity, therefore we investigated various methods of calculating the product first of all.The following methods were studied:

— A1 – "School" method – it is provided for comparison and verification of the results correctness;

— A2 – Toom-Cook's algorithm. It is implemented according to the [3] recommendations. Even without interpolation, time characteristics are worse than the rest of the algorithms;

— A3 – FFT, Fast Fourier transform (algorithm with pre-calculations). Time characteristics approximately coincide with the time characteristics for the Toom-Cook's algorithm;

— A4 – Our algorithm that takes into account the special structure of a polynomial with coefficients (0, -1, 1) for which numbers are given, using AVX2 commands;

— A5 – Algorithm A4, which uses 2 threads.

— A6 – Algorithm A4, which uses 4 threads.

The results of the experimental research for some parameters from NTRU Prime are shown in Table 2 The first column defines the parameter number in the Table B Parameters [3].

Table 2

N	A1	A2	A3	A4	A5	A6
439	403796	152191	143679	40179	26588	18436
457	451344	157148	147812	37692	26336	18492
461	459088	157196	148476	46116	29808	20212
461	459120	157064	148352	46188	27444	20008
467	471340	157100	148196	24852	17636	14556
463	462736	157196	148268	40900	24724	18864
463	462828	156972	148608	43312	28768	19700
463	462676	157164	148460	46788	30672	20220
479	494224	157144	148020	36664	22468	18096
479	494156	157204	148228	39408	26168	18236
491	519168	157096	148556	41048	25784	19084

Conclusions on the multiplication methods:

1. The usage of complex algorithms (A2, A3) that do not take into account special structure of the polynomial with coefficients (-1, 0, 1) makes no sense.

2. The polynomial with coefficients (-1, 0, 1) is better to be specified using non-zero elements indices (A4, A5, A6).

3. The use of threads in case of modulus reduction on the multicore processor makes sense.

After completing the multiplication operation, we obtain the polynomial, coefficients of which don't exceed $q*n$, and the polynomial degree is $2n-1$. This polynomial must first be reduced by modulus $x^n - x - 1$, after that we obtain the polynomial of n-degree, and then each of n coefficients are reduced by modulus q.

3 Reducing by modulus $x^n - x - 1$ optimization

For reduction by modulus $x^n - x - 1$ it is sufficient to polynomial coefficients with indices $0 \ldots n-1$ to add (subtract) corresponding coefficients with indices $n \ldots 2n-2$.

To simultaneously reduction the coefficients block using AVX2 operations.

4 Reducing by the modulus q – Barrett reduction optimization

To accelerate the method, the constants, which depend only on the values of n, q, are computed ones when setting parameters [9].

Barrett bk, bc constants pre-calculation:

$$bk \text{ is chosen such that } 2^{bk} > p*q; \quad (3)$$

$$bc = 2^{bk} / q \text{ is calculated.}$$

For each polynomial coefficient h_i, it must perform the following calculations:

$$h_i = h_i - ((h_i * bc) >> bk) * q. \quad (4)$$

To simultaneously reduction by modulus q the coefficients block using AVX2 operations.

5. Optimization of Blinding polynomial calculation algorithm

Blinding polynomial calculation is performed according to the Blinding Polynomial Generation Method (BPGM) – Algorithm 18 [1]. The algorithm uses the index generation function (IGF) by which the bit string (IGF state s) creates, with the length $minCallsR * Hlen$ (see Algorithm 20 [1]). When implementing the creation function s, a constant part is formed that is used at each step of the calculation of the hash. When forming a hash, AVX2 commands are used.

To optimize the calculation of polynomial coefficients in the first step, an array of coefficients is formed fully. At the second step, the possibility of their application is checked. If necessary, the bit string expands.

5.1. Optimization of IGF state *s* formation

For option 1, use of the hash function as proposed in the standard [1]. To optimize the implementation of the *s* creation function, a constant part is formed that is used at each step of the hash value calculation. When forming a hash value, AVX2 commands are used.

For option 2, when implementing the *s* creation function, the initial string and its length are defined as for option 1, but instead of multiple recalling of the hash function, the multiple encryption function call for the SALSA-20 algorithm is used [7]. For the next step of encrypting, the result for the previous step is selected. The number of steps compared to the algorithm for option 1 is reduced due to the fact that the length of the initial state is longer than the length of the hash value.

For option 3, instead of the function for algorithm SALSA-20, the encryption function for the SNOW-20 algorithm is used [4].

5.2. Coefficients calculation optimization

To optimize the calculation of the polynomial coefficients in the first step, a completely array of coefficients is formed. At the second step, the possibility of their application is checked. If necessary, the bit string is expanded.

Blinding polynomial is used for data encryption and decryption. The effect of various methods of blinding polynomial formation is shown in table 3.

6. MGF algorithm optimization

The algorithm uses the $minCallMask$ parameter (see Algorithm 19 [1]) to generate a bit string. The bit string formation optimization is made due to the fact that the constant part is used at each step of the hash calculation is calculated only once. When forming a hash, AVX2 commands are

used. For fast conversion of a byte string into a polynomial, a pre-computed table is used, the entry point of which is byte and each row includes 5 coefficients.

7. Encryption algorithm optimization

In the encryption algorithm 2 branches are executed in parallel. The first branch includes Steps 4-8 of the encryption algorithm (Algorithm 23 [1]). The second branch includes Steps 9-10 (Algorithm 23 [1]). To implement parallel branches, the Open MP parallelization standard is used [8].

The encryption algorithm coincides with Algorithm 23 (ANSI X 9.98 [1]). Next, the notation is used from Algorithm 23.

1. For strings M and $sData$, intersecting memory is used. This allows you to reduce the amount of memory required by the message length and reduce the time it takes to copy the string for encryption (Step 5 and Step 9).

2. To accelerate the formation of $Mtrin$ (Step 8), the bit string is processed in portions of 3 bytes, which allows you to immediately get 8 polynomial coefficients. The case is handled correctly when the length of the string is not multiple 3.

3. To exclude the need to convert a public key into a byte string (Step 9), it is stored in the container in the form of a byte string and in the form of a polynomial.

4. For blinding polynomial generation (Step 10) a BPGM method is used, which optimization will be described above (see 5).

5. To calculate $r*h$ (Step 11), the multiplication function is used for one or multi-core processor according to the execution environment. The maximum number of cores that the function uses is 4.

6. Step 12 and Step 13 are executed as one step.

7. The polynomial generation to mask $mask$ (Step 14 of Algorithm 19 [1]).

8. Steps 15-18 are executed as one step in which the modules are formed and the numbers of values -1, 0, 1 are calculated, their correctness is checked and the ciphertext value is calculated.

9. The result is an array of bytes that we obtain by converting a polynomial into an array of bytes according to the package algorithm. To optimize the latter, separate algorithms are developed, depending on the bit length q.

8. Decryption algorithm optimization

The decryption algorithm is executed according to Algorithm 24 [1]. Next, the notations are used from Algorithm 24.

1. Steps 1-3 are combined in one step. The multiplication algorithm A4–A6 is used to multiply polynomials depending on the number of processor cores. The number of non-zero elements of received polynomial is counted simultaneously with its formation.

2. Steps 4-6 are combined in one step, that allows to form in one cycle a byte row to calculate $c0R4$.

3. Step 7 optimization (see paragraph 6).

4. To optimize Step 8, the cycle is deployed to simultaneously receive 4 bytes of string.

5. Steps 9, 10, 11 are combined in one step. That allowed in one cycle to form a byte string.

6. Step 12 of the algorithm actually determines the message after the decryption. Further, the "speculative" execution of the code that uses these data may be continued. The following steps can be performed in parallel with the use of the obtained data. If in result of additional checks will be obtained a negative result, the code execution after the use of decrypted data should be determined to be invalid. In case of successful additional verification, the executed code is accepted as valid. Additional checks include Steps 13-17.

7. For Step 13, you do not need to convert the public key into a byte string, it is stored in this format.

8. Step 14 optimization to form a blinding polynomial (see paragraph 5).

9. Step 15 polynomials multiplying.

9. Time rates of encryption and decryption functions

The results of the experimental research for some parameters from NTRU Prime are shown in Table 3. The first column defines the parameter number in the Table B Parameters [3]. Number ring from 0. Parameter № 64 (n=739, q=9829) is given for comparison with the data given in [3]. Parameter №74 (n=761, q=4591) is chosen for comparison with the data given in [5].

Table 3

№	*N*	*Q*	Encrypt			Decrypt			Decrypt	
			Hash	Salsa20	Snow20	Hash	Salsa20	Snow20	Decrypt	Check
0	439	6833	56364	40456	35408	81356	64280	60016	29048	28508
1	457	6037	62712	38200	33712	87948	61448	56868	30500	28496
4	467	3911	52340	32016	29252	72760	51528	48532	26908	23320
5	463	6529	64336	39124	35288	90484	63256	59072	32352	29220
6	463	6841	66240	40628	36268	94884	66448	61464	32336	30884
8	479	5689	62800	38396	34144	87748	61556	57320	31000	28360
9	479	6089	64444	39072	34796	90624	62596	58352	32168	28948
10	491	6287	67464	41304	36188	94220	65984	61500	31368	30600
15	503	2879	50460	30536	27844	87748	61556	47116	31000	28360
17	523	3331	54192	33112	30812	90624	62596	51224	32168	28948
64	739	9829	104916	61597	53876	145516	100152	93224	48636	46488
74	761	4591	73456	44120	40032	100140	71480	67728	37580	30920

For encryption and decryption operations, there are 3 modes for creating a random string to create a blinding polynomial (hash, salsa20, snow20), see paragraph 5. For both functions, we get the best results for the last mode.

The last 2 columns determine the time taken to decrypt and verify the decryption correctness. In the case of parallel execution of the verification operation with other encryption-decryption operations, you can balance the time required for encryption and decryption.

The last row in the table specifies the results obtained for the parameters specified in [5]. These parameters correspond to a cryptographic stability of more than 200.

Authors [5] received the results:

Encryption: 59600 and decryption 97452 cycles respectively.

In the case of the hash value using, our encryption operation implementation loses the specified ones in the by 25%, and the decryption operation – 5%. When using SNOW 2.0, our implementation wins 30% for encryption algorithm and 29% for decryption algorithm.

In [6] – one of the algorithms submitted to the competition (Kyber), the following performance data after optimization using AVX2 are given:

Encryption – 119652;

Decryption – 125736.

Compared to our results for the best option, we get the winning: 65% for encryption and 44% for decryption.

Conclusions

According to the results of the work we can made the following conclusions:

1. During optimization great attention was paid to multiplication operation, as it is the most time consuming. Usage of complex multiplying algorithms, which don't take into account special polynomial structure with coefficients (-1, 0, 1) doesn't make sense. The polynomial with coefficients (-1, 0, 1) is better to be specified using non-zero elements indices. The use of threads in case of reduction by modulus on the multi-core processor makes sense. Usage of AVX2 operations for reduction by modulus polynomial $x^n - x - 1$ and prime q and for Barrett algorithm for reduction by modulus q are effective and accelerates multiplication speed.

2. Blinding polynomial generation, coefficient calculation, blinding polynomial generation and index generation function optimizations were also made.

3. Encryption and decryption algorithms were optimized due to the parallel computing.

4. Three algorithms of blinding polynomial formation were studied (hash, salsa20, snow20), the best time rates were obtained for Snow 2.0.

5. In case of usage encryption algorithms our implementation wins 30 % for encryption algorithm and 29 % for decryption algorithm.

6. Compared to the data given in [6], we have got the winning: 65 % for encryption and 44% for decryption.

References: 1. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. – 2010. 2. Electronic resource: https://csrc.nist.gov/projects/post-quantum-cryptography. 3. *Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch.* NTRU Prime // Cryptology ePrint Archive: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf. 4. *Patrik Ekdahl, Thomas Johansson*. A New Version of the Stream Cipher SNOW // SAC 2002: Selected Areas in Cryptography pp 47-61. 5. *Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van redendaal*. NTRU Prime: reducing attack surface at low cost // Cryptology ePrint Archive: https://eprint.iacr.org/2016/461. 6. *Joppe Bos, Leo Ducas, Eike Kiltz*. CRYSTALS – Kyber: a CCA-secure modulus-lattice-based KEM // https://eprint.iacr.org/2017/634. 7. *Daniel J. Bernstein.* Salsa20 design // https://cr.yp.to/snuffle/design.pdf 8. Electronic resource http://www.openmp.org/. 9. P D Barrett, "Communications Authentication and Security using Public Key Encryption – A Design for Implementation." (Oxford University Programming Research Group MSc Thesis (1984).

Харьковский национальный
университет радиоэлектроники,
Акционерное общество
«Институт информационных технологий»,
Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 10.10.2017

УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, О.Г. КАЧКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук

АНАЛІЗ АЛГОРИТМУ НАПРАВЛЕНОГО ШИФРУВАННЯ NTRU PRIME IIT UKRAINE З УРАХУВАННЯМ ВІДОМИХ АТАК

Вступ

У 2016 – 2017 роках відбувся ряд значущих подій, які уже суттєво вплинули на інтенсивний розвиток постквантової криптографії. До них слід віднести статтю Alfred J. Menezes та Neal Koblitz [2], організацію та проведення NSA та NIST США VII міжнародної конференції з постквантової криптографії [5, 6]. Надзвичайно важливою подією стало опублікування в США звіту «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT)» [3], в якому було підтверджено можливості успішного квантового криптоаналізу асиметричних криптосистем електронного підпису (ЕП), а також визначені основні проблеми та можливості і етапи їх вирішення.

NIST США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів ЕП та асиметричного направленого шифрування (НШ), які будуть актуальними та можуть застосовуватись у постквантовий період, оголосив конкурс на розробку стандартів постквантових асиметричних криптографічних примітивів [5]. Вказане обумовлено двома факторами. По-перше, спостерігається помітний прогрес у розвитку квантових комп'ютерів, у тому числі проводяться експериментальні демонстрації реалізації фізичних кубітів, які можуть бути масштабовані до більших систем. Підтвердженням цьому є послідовний анонс IBM 20, 50 та 53 – кубітних квантових комп'ютерів [26, 27].

По-друге, скоріше всього перехід до постквантової криптографії не буде простим, оскільки навряд чи буде простою заміна поточних стандартів асиметричних криптографічних примітивів. Значні зусилля будуть потрібні для того, щоб розробити, стандартизувати та впровадити нові постквантові криптосистеми. Тому повинен бути значний перехідний етап, коли будуть застосовуватись як нинішні, так і постквантові криптографічні примітиви.

Заявки отримувались NIST до 30 листопада 2017 року. Вони стосуються: асиметричних алгоритмів НШ та ЕП. В подальшому очікується їх детальний аналіз та порівняння, причому на це відводиться період до трьох років. Вказане свідчить про суттєву складність проблеми, що має бути вирішена.

Європейський союз також розпочав активну роботу з підготовки нових постквантових стандартів. Європейською організацією зі стандартизації ETSI сформований новий напрямок «Квантово-захищена криптографія» [1, 4, 7]. За результатами даних досліджень прогнозується прийняття групи стандартів для постквантового періоду. ETSI опублікувала груповий звіт «Квантово-захищена криптографія. Квантово-безпечна інфраструктура» [1], в якому закріплено основи перспективної інфраструктури, представлено алгоритми, описано типи примітивів, що будуть використовуватися. Окремо висунуто вимоги та сформовано критерії оцінки майбутніх кандидатів.

За участі авторів цієї статі на конкурс, що проводиться NIST США, подано криптографічний алгоритм НШ «NTRU Prime IIT Ukraine» [10], який розроблено з використанням NTRU [8] та NTRU Prime [9]. Метою цієї статі є загальний огляд та опис запропонованого криптоперетворення, особливості реалізації, оцінка та порівняння основних характеристик та показників з [8 – 10] за критеріями криптографічної стійкості від існуючих та потенційно можливих атак.

1. Постановка проблеми

На основі аналізу джерел [8, 9] стосовно існуючих на сьогоднішній день алгоритмів НШ, їх особливостей, переваг та недоліків, а також стійкості до атак було визначено, що на їх основі можливо створити новий алгоритм НШ, який буде поєднувати головні переваги існуючих та не буде мати певних недоліків. В результаті широких досліджень обґрунтовано

сутність кандидату, розроблено його реалізації, що мають переваги відносно відомих, зроблено випробовування та оцінки основних характеристик. У листопаді 2017 року повний комплект опису проекту та програмні реалізації були надіслані та отримані NIST США [5]. Вважається за необхідне статтю розглядати як перший етап попереднього дослідження нашої пропозиції та ознайомлення широкого загалу з проблемою створення постквантового стандарту асиметричного НШ. Таким чином, метою цієї статі є обґрунтування та викладення основних ідей побудови постквантового стандарту асиметричного НШ, аналізу стану робіт в указаному напряму, викладення сутності відмін пропозиції «NTRU Prime IIT Ukraine» від відомих, а також обговорення результатів оцінки та випробовування стосовно вимог, що висунуті NIST США.

Аналіз вимог до постквантових криптоперетворень асиметричного шифрування дозволяє зробити висновок, що основною, причому безумовною вимогою щодо «NTRU Prime IIT Ukraine», є вимога криптографічної стійкості щодо відомих та потенційно можливих атак. Вказані атаки можуть бути реалізовані з використанням як класичних атак на основі використання класичних комп'ютерних систем та класичних математичних методів, а також на основі квантових комп'ютерів та відповідних математичних і програмних методів. Очевидно, що криптографічні асиметричні перетворення, повинні забезпечувати захист як від класичних, так і квантових методів криптоаналізу. Вказане повинне враховуватись, по можливості, при побудуванні та аналізі постквантових криптоперетворень, прийнятті на їх основі постквантових стандартів асиметричних криптоперетворень.

2. Опис та аналіз загальних параметрів сучасних NTRU-подібних алгоритмів НШ

Розглянемо далі існуючі сьогодні алгоритми направленого шифрування та створений на їх основі новий алгоритм направленого шифрування «NTRU Prime IIT Ukraine» [8 – 10].

Аналіз алгоритму шифрування NTRU. NTRU – перша криптографічна система відкритого ключа, яка не ґрунтується на факторизації чи проблемі дискретного логарифмування. NTRU ґрунтується на проблемі найкоротшого вектору в решітці. Операції ґрунтуються на об'єктах в зрізаному кільці поліномів $R = \mathbf{Z}[x]/(x^n - 1)$, степінь полінома не більше $n-1$.

Параметрами NTRU є наступні: n – поліноми у кільці R мають ступінь $n-1$ (не таємний); q – великий модуль, за яким зводиться кожний коефіцієнт (не таємний); p – малий модуль, за яким зводиться кожний коефіцієнт (не таємний); f – поліном, що є секретним ключем; g – поліном, який використовується для генерації відкритого ключа h з f (секретний, але відкидається після початкового використання); h – відкритий ключ, також поліном; r – випадковий "засліплюючий" поліном (секретний, але відкидається після початкового використання); d – коефіцієнт.

Зашифрування відкритого повідомлення m здійснюється за формулою $c = rh + m$.

Розшифрування виконується наступним чином: з використанням особистого полінома f обчислюється поліном $a = f \cdot e (\mathrm{mod}\, q)$. Далі обчислюється поліном $b = a \bmod p$. Використовується ще один особистий поліном f_p для обчислення $c = f_p \cdot b (\mathrm{mod}\, p)$, де c і є вихідним повідомленням m.

Більш детально про алгоритм NTRU описано у [8].

3. Аналіз алгоритму шифрування NTRU Prime

Криптосистема NTRU Prime запропонована як один з альтернативних варіантів асиметричного методу NTRU з метою позбутися слабких місць, притаманних NTRU, які пов'язані з небажаними структурними властивостями кільця $\mathbf{Z}_q[x]/(x^n - 1)$: у багатьох випадках кільце такого виду має підкільця та фактор кільця великого порядку. На відміну від NTRU, в NTRU Prime використовується кільце $\mathbf{Z}_q[x]/(x^n - x - 1)$, яке за умови належного вибору чисел q і

n, є полем, що не містить власних підполів. Крім того, група Галуа полінома $x^n - x - 1$ над полем Q є симетричною групою S_n, що виключає можливість проведення на криптосистему атак певного виду.

У NTRU Prime відкритий ключ обчислюється за формулою $h = g / 3f$, що має значення для створення ефективного протоколу передачі секретних ключів. Однак для побудови асиметричної шифрувальної системи бажано використовувати традиційну формулу $h = 3g / f$.

Розшифрування повідомлень у криптосистемі NTRU Prime відбувається коректно за умови $q > 48t$.

Детальніше про алгоритм NTRU Prime описано у [9].

4. Аналіз алгоритму шифрування NTRU Prime IIT Ukraine

Дане асиметричне криптоперетворення являє собою модифікацію криптоперетворення NTRU та відрізняється від останнього лише двома аспектами:

1. Замість кільця $\mathbf{Z}_q[x]/(x^n - 1)$, що використовується в NTRU, застосовується поле $\mathbf{Z}_q[x]/(x^n - x - 1)$, як у криптосистемі NTRU Prime [9]. Згідно з [9] це унеможливлює проведення на криптосистему атак деякого виду та виключає можливість скористатися (принаймні, потенційними) слабкостями стандартної криптосистеми NTRU, які пов'язані з існуванням нетривіальних підкілець чи факторкілець кільця $\mathbf{Z}_q[x]/(x^n - 1)$.

2. У запропонованому криптоперетворенні поліноми F та r є довільними t-малими, тобто мають $2t$ ненульових коефіцієнтів, які дорівнюють ± 1, в той час як в [8] кожен з зазначених поліномів має точно t ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно. Аналогічне зауваження справедливе і для полінома g, який є довільним малим поліномом у модифікованій криптосистемі та має однакову кількість ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно в NTRU. Ця відмінність не є суттєвою, проте надає можливість розширити обсяг ключового простору в порівнянні з NTRU без втрати ефективності реалізації алгоритмів формування ключів та зашифрування-розшифрування повідомлень.

У даному алгоритмі секретним ключем є будь-яка пара поліномів (f, g), де $f = (1 + 3F) \bmod q$, $F, g \in R/3$, $\| F \|_1 = 2t$, а відповідним відкритим ключем – поліном $h = 3g / f \in R/q$.

Зашифрування відкритого повідомлення m здійснюється за формулою $c = m + rh$, де r – випадковий рівноймовірний t-малий поліном, h – відкритий ключ, а додавання та множення здійснюються в полі R/q.

Для відновлення повідомлення m за повідомленням c за допомогою секретного ключа (f, g), слід обчислити $m' = (cf \pmod q) \bmod 3$ та покласти $m'' = (m' f^*) \bmod 3$. Тобто, для розшифрування повідомлень використовуються тільки поліноми f та f^*, де f^* є оберненим до елемента $f \bmod 3$ в кільці $R/3$.

У «NTRU Prime IIT Ukraine» за допомогою відповідних оцінок, що вказані в описі алгоритму, можна (дозволяється) помітно послабити умову щодо розшифрування повідомлень порівняно з NTRU Prime, а саме, замінити її умовою $q > 32t$. А це, в свою чергу, надає можливість зменшити значення q порівняно з NTRUPrime, зберігаючи при цьому коректність розшифрування.

Більш детально алгоритм «NTRU Prime IIT Ukraine» описано у [10].

5. Аналіз алгоритму з урахуванням відомих атак щодо «NTRU Prime IIT Ukraine»

Проведемо аналіз стійкості алгоритму направленого шифрування «NTRU Prime IIT Ukraine» [10] щодо відомих атак.

Атака «зустріч посередині»

Зазначимо, що дана атака на сьогодні реалізується на звичайних комп'ютерах, але безумовно, можлива її реалізація і на квантових комп'ютерах.

Задача відновлення секретного ключа $(f = (1+3F) \bmod q, g)$ за відкритим ключем h криптосистеми зводиться до розв'язання рівняння $(h' + Fh') \bmod q = g$ відносно невідомих $F, g \in R/3$, де $\| f \|_1 = 2t$ і $h' = (3^{-1}h) \bmod q$. Цю задачу можна сформулювати таким чином.

Нехай $\Phi = \{F \in R : \| F \|_\infty = 1, \| F \|_1 = 2t\}$. Треба знайти поліном $F \in \Phi$ такий, що

$$\| (h' + h'F) \bmod q \|_\infty = 1. \tag{1}$$

Трудомісткість розв'язання поставленої задачі шляхом повного перебору всіх поліномів $F \in \Phi$ потребує $|\Phi| = 4^t \binom{n}{2t}$ операцій. Для зменшення трудомісткості можна застосувати атаки під загальною назвою «зустріч посередині».

Опишемо загальну схему побудови таких атак, базуючись на ідеях робіт [11, 13, 14].

Задамо множини $\Phi_1, \Phi_2 \subseteq \mathbf{Z}^n$ такі, що кожен вектор $F \in \Phi$ має єдине представлення у вигляді $F = F_1 + F_2$, де $F_1 \in \Phi_1$, $F_2 \in \Phi_2$, та певне відображення $D : Z_q{}^n \to \{0,1\}^r$, де $r \le n$.

Алгоритм розв'язання рівняння (1) відносно невідомого $F \in \Phi$ складається з двох етапів, на першому з яких будується таблиця, яка складається з усіх пар $(h'F_1 (\bmod q), D(h'F_1 (\bmod q)))$, розташованих за незростанням цілих чисел, що відповідають двійковим векторам $D(h'F_1 (\bmod q))$, де $F_1 \in \Phi_1$. Потім, на другому етапі для кожного $F_2 \in \Phi_2$ відбувається пошук вектора $D(-h' - h'F_2 (\bmod q))$ серед других компонент пар, які знаходяться в побудованій таблиці. Алгоритм завершується успішно в разі знаходження векторів $F_1 \in \Phi_1$, $F_2 \in \Phi_2$ таких, що $D(h'F_1 (\bmod q)) = D(-h' - h'F_2 (\bmod q))$ та $\| (h' + h'(F_1 + F_2)) \bmod q \|_\infty = 1$.

Зауважимо, що в [9, 11, 13, 14] для різних варіантів криптосистеми NTRU наводяться евристичні оцінки трудомісткості атак зустріч посередині, які базуються на явних чи неявних припущеннях відносно відображення D та розподілу векторів у таблиці, яка будується на першому етапі. Поряд з тим, незалежно від вибору відображення D максимальна трудомісткість описаного алгоритму обмежена знизу значенням $|\Phi_1| + |\Phi_2| \ge 2\sqrt{|\Phi_1||\Phi_2|}$, яке, у свою чергу, є не менше ніж $2\sqrt{|\Phi|} = 2^{t+1} \binom{n}{2t}^{1/2}$.

Таким чином, для забезпечення стійкості криптосистеми «NTRU Prime IIT Ukraine», відносно атак «зустріч посередині» значення n і t вибираються для заданого параметра безпеки k, виходячи з умови

$$2^k \le 2^{t+1} \binom{n}{2t}^{1/2}. \tag{2}$$

Розглянемо надалі атаки в плані їх стійкості при застосуванні квантових алгоритмів [8, 20 – 24], причому спочатку розглянемо атаку «зустріч посередині».

Нехай B – множина булевих багаточленів ступеня N. Також нехай $B(d)$ – підмножина B, багаточлен якого має d коефіцієнтів 1, і $N-d$ коефіцієнтів 0. $T(d+,d-)$ – множина багаточленів, де число коефіцієнтів 1 дорівнює $d+$, а число коефіцієнтів –1 дорівнює $d-$, а інші є 0.

Атака «зустріч посередині» дозволяє при певних умовах криптоаналітику обчислити особистий ключ користувача обраного з простору 2^N елементів за час $O\left(2^{N/2}\right)$. Запропонована атака реалізується наступним чином [9]. Простір особистих ключів ($f=(1+pF) mod\ q$) f розділяється на дві великі частини $f_1 \| f_2$, де f_1 та f_2 мають довжину $N/2$ з $d/2$ одиниць кожен, причому однакове число одиниць досягається циклічним зсувом f при діленні на дві частини. За даної умови на основі ($h = p(f_q^{-1} * g)\ mod\ q$), при $p = 2$, виконується умова, що:

$$f \cdot h = g (\mathrm{mod}\, q) \tag{3}$$

Підставивши замість f його подання у вигляді $f_1 \| f_2$ маємо, що

$$(f_1 \| f_2) \cdot h = g (\mathrm{mod}\, q) \tag{4}$$

Порівняння (4) можна подати у вигляді

$$f_1 \cdot h = g - f_2 \cdot h (\mathrm{mod}\, q) \tag{5}$$

На останок (5) можна подати у вигляді

$$(f_1 \cdot h)_i = \{1,0\} - (f_2 \cdot h)_i (\mathrm{mod}\, q) \forall i \tag{6}$$

Фактично для f може і не виконуватися умова, що половина одиниць попадає в перші $N/2$ записів. Як показано в роботі [23], існує хоча б одне крутіння f, яке буде задовольняти цій властивості, а в якості особистого ключа буде будь-яке крутіння f.

За вказаних умов атака складається з наступних кроків.

1. Визначається число k, яке задовольняє умові:

$$2^k \geq \binom{N/2}{d/2} \tag{7}$$

Далі виділяється пам'ять під 2^k корзин для зберігання багаточленів. Чим більшим буде обрано k, тим швидше буде виконуватися алгоритм, але потрібно буде більше пам'яті.

2. До багаточлену f_1 додається $N/2$ нулів та здійснюється їх перебирання. Перебір займе $\binom{N/2}{d/2}$ кроків. Кожне значення f_1 записується до корзини таким чином, щоб номер корзини, в яку буде поміщатися багаточлен, дорівнював найбільш значимим бітам перших k коефіцієнтів $f \cdot h = g (\mathrm{mod}\, q)$. Позначимо кожну корзину, як $label\_f_1$. При цьому, в деяких корзинах буде по декілька значень багаточленів.

3. Далі аналогічно перебираються багаточлени f_2 та формуються корзини $label\_f_2$, але нульові біти додаються до початку. Сформований багаточлен розміщується до корзин, номер яких формується наступним чином – найбільш значимі біти для перших k коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$, а також найбільш значимі біти для перших k коефіцієнтів багаточлену $-f_2 * h (\mathrm{mod}\, q)$ до кожного коефіцієнту якого додається 1.

4. У випадку, якщо при записі f_2, в корзині є багаточлен f_1, то він вважається добрим кандидатом для відновлення f. Криптоаналітик обчислює $(f_1 \| f_2)\cdot h = g(\mathrm{mod}\, q)$. Якщо він складається з $\{0,1\}$, то особистий ключ знайдено.

Таким чином, при здійсненні атаки з застосуванням методу типу «зустріч посередині» встановлено, що цей алгоритм завжди може повернути результат, який, швидше за все, є особистим ключем f, або циклічним зсувом f.

Згідно [25] часова та просторова складності атаки «зустріч посередині» можуть бути оцінені як

$$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}}), \tag{8}$$

У цілому (8) дозволяє оцінити складності часової та просторової атаки на алгоритм NTRU. Отримані вище співвідношення можна використати для порівняння складності атаки «повне розкриття» з атаками на основі квантових алгоритмів.

Атака на решітках

Відмітимо, що даний тип атак реалізується на звичайних комп'ютерах, але також у майбутньому можлива його реалізація і на квантових комп'ютерах.

Для будь-якого $h \in R/q$ позначимо $L(h)$ решітку у векторному просторі R^{2n+1}, породжену рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times n} & h' \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}, \tag{9}$$

де I_n – одинична матриця порядку n, H – $n\times n$-матриця, i-й рядок якої дорівнює вектору коефіцієнтів полінома $(x^i h) \bmod (x^n - x - 1)$, $i \in \overline{0, n-1}$, $h' = (3^{-1} h) \bmod q$, 3^{-1} – елемент кільця R/q, обернений до 3:

$$3^{-1} = (5+q)/6, \text{ якщо } q \equiv 1 \bmod 3;\ \ 3^{-1} = (5-q)/6, \text{ якщо } q \equiv -1 \bmod 3.$$

Наступне твердження уточнює (для випадку криптосистеми, що розглядається) основний результат роботи [15].

Твердження 1. Якщо вектор $(f = (1+3F) \bmod q, g)$ є секретним ключем криптосистеми, якому відповідає відкритий ключ h, то

$$(1, F, g) \in L(h) \tag{10}$$

та

$$\| (F,g) \|_2 = \left(\sum_{i=0}^{n-1} |F_i|^2 + \sum_{i=0}^{n-1} |g_i|^2 \right)^{1/2} \le \sqrt{n+2t}\,. \tag{11}$$

З іншого боку, якщо вектор (F, g) задовольняє умові (10) та має довжину

$$\| (F,g) \|_2 < \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}, \tag{12}$$

то за допомогою вектора $f = (1+3F) \bmod q$ можна відновити будь-яке вхідне повідомлення m за повідомленням $c = E_h(m,r)$, вважаючи $m = (cf \,(\bmod q)) \bmod 3$.

Доведення. Перша частина твердження випливає безпосередньо з наведених означень.

Для доведення другої частини розглянемо криптограму $c = (m+rh) \bmod q$, отриману в результаті перетворення вхідного повідомлення $m \in R/3$ за допомогою відкритого ключа h і t-малого полінома r.

На підставі умови (10) справедлива рівність $(3g) \bmod q = (fh) \bmod q$. Зауважимо, що $f \neq 0$, оскільки в протилежному випадку $F = 3^{-1}$, $g = 0$ $\| (F,g) \|_2 \geq \frac{q-5}{6} > \frac{q-2}{12(\sqrt{n}+\sqrt{2t})}$, оскільки $q > 48$, що протирічить умові (12).

Використовуючи оцінку ($\| uv \|_\infty \leq 2 \| u \|_\infty \| v \|_1$) та формулу (12), отримаємо, що

$$\| mf + 3rg \|_\infty \leq \| m \|_\infty + 3(\| mF \|_\infty + \| rg \|_\infty) \leq 1 + 6(\| m \|_2 \| F \|_2 + \| g \|_2 \| r \|_2) \leq$$

$$\leq 1 + 6(\| m \|_2 + \| r \|_2) \| (F,g) \|_2 \leq 1 + 6(\sqrt{n}+\sqrt{2t}) \| (F,g) \|_2 < q/2 .$$

Звідси випливає, що $(cf) \bmod q = (mf + 3rg) \bmod q = mf + 3rg$ і, отже,

$$(cf \,(\bmod q)) \bmod 3 = (mf + 3rg) \bmod 3 = (m(1+3F)) \bmod 3 = m .$$

Твердження доведено.

Таким чином, задача відновлення секретного ключа криптосистеми за її відкритим ключем h зводиться до пошуку достатньо короткого вектора (з першою координатою, що дорівнює одиниці) в решітці $L(h)$. Приймаючи звичайне евристичне припущення, що шуканий вектор є найкоротшим ненульовим вектором решітки $L(h)$, приходимо до висновку, що відновлення секретного ключа рівносильно розв'язанню задачі про найкоротший вектор (shortest vector problem (SVP)) для цієї решітки. Зауважимо, що остання задача рівносильна знаходженню вектора, найближчого до вектора $(0_{1\times n}, h')$, у решітці, породженої рядками матриці $\begin{pmatrix} I_n & H \\ 0_{n\times 1} & qI_n \end{pmatrix}$ (closest vector problem (CVP)).

Задача обернення функції E_h або, що рівносильно, відновлення вхідного повідомлення $m \in R/3$ за вихідною криптограмою $c = (m+rh) \bmod q$, де $r \in R/3$, $\| r \|_1 = 2t$, також зводиться до пошуку найкоротшого (або достатньо короткого) вектора решітки $L(h,c)$, породженої рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times n} & c \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}.$$

Обидві решітки $L(h)$, $L(h,c)$ мають однаковий вигляд та відносяться до класу модулярних решіток.

Гібридна атака

Слід вказати, що ця атака реалізується на звичайних комп'ютерах, але також можлива її реалізація у майбутньому і на квантових.

Гібридна атака на класичну криптосистему NTRU запропонована в [13] і в подальшому досліджувалась в багатьох публікаціях. Певним підсумком цих досліджень можна вважати роботу [16], де показано, що оцінки трудомісткості гібридної атаки, отримані раніше для різ-

них криптосистем, є дуже неточними внаслідок помилкових припущень та сумнівних евристичних міркувань, що використовуються для отримання цих оцінок.

Зауважимо, що в [16] також використовуються певні евристичні припущення, тому питання про строго обґрунтовані оцінки трудомісткості гібридної атаки є предметом подальших досліджень.

Стосовно криптосистеми, що розглядається, гібридна атака здійснюється таким чином [16].

Розглянемо решітку $L(h)$, породжену рядками матриці (9), зафіксуємо число $r \in \overline{1, n-1}$ та запишемо матрицю H у вигляді $H = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$, де H_1 та H_2 є цілочисельними матрицями розміру $r \times n$ та $(n-r) \times n$ відповідно. Довільний вектор $F \in Z^n$ будемо записувати у вигляді $F = (F_1, F_2)$, де $F_1 \in Z^r$, $F_2 \in Z^{n-r}$.

Помітимо, що вектор $(1, F, g)$ належить решітці $L(h)$ тоді й тільки тоді, коли існує вектор $x \in Z^n$ такий, що

$$F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) = -(1, F_2, x)\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix} + (1, F_2, g). \qquad (13)$$

Остання рівність рівносильна тому, що вектор $F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1) - (1, F_2, g)$ належить решітці $L_r(h)$, породженої рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times(n-r)} & h' \\ 0_{(n-r)\times 1} & I_{n-r} & H_2 \\ 0_{n\times 1} & 0_{n\times(n-r)} & qI_n \end{pmatrix}.$$

Згідно з [16], гібридна атака залежить від параметрів r, l, c_{-1}, c_1 і спрямована на знаходження вектора $(1, F_1, F_2, g) \in L(h)$, який задовольняє таким умовам:

а) F_1 є малим вектором, що має точно $2c_{-1}$ координат, які дорівнюють -1, та $2c_1$ координат, які дорівнюють 1;

б) (F_2, g) є малим вектором, що має евклідову норму l.

Атака складається з двох етапів, на першому з яких тим чи іншим чином будується редукований базис B решітки $L_r(h)$. Далі, на другому етапі, перебираються вектори F_1, що задовольняють умові (а), за якими обчислюються вектори $(v, F_2, g) = \mathrm{NP}_B(\hat{F}_1)$, де $v \in Z$, а $\mathrm{NP}_B(\hat{F}_1)$ позначає результат застосування до вектора $\hat{F}_1 = F_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$ та базису B решітки $L_r(h)$ алгоритму Бабаї. Зазначений алгоритм знаходить «достатньо короткий» вектор $e = \mathrm{NP}_B(\hat{F}_1)$, для якого $\hat{F}_1 - e \in L$, за умови, що базис B є «достатньо добре» редукованим [17].

З рівності (13) та умови (б) випливає, що вектор $\hat{F}_1$ є близьким до решітки $L_r(h)$, тому природно шукати найближчий до нього вектор цієї решітки у вигляді $\hat{F}_1 - \mathrm{NP}_B(\hat{F}_1)$. Крім того, на підставі рівності (13) для будь-якого $F_1 \in Z^r$ вектор $(1, F_1, F_2, g)$ належить решітці

$L(g)$, якщо $\mathrm{NP}_B(\hat{F}_1)=(1,F_2,g)$. Тому все, що залишається перевірити для вектора $\mathrm{NP}_B(\hat{F}_1)$ на другому етапі атаки, є рівність $\nu=1$ та умова (б).

Для того щоб пришвидшити пошук векторів на другому етапі, застосовується метод «зустрічі посередині»: замість векторів F_1, що задовольняють умові (а), перебираються малі вектори f_1 довжини r, кожний з яких має точно c_{-1} координат, що дорівнюють -1, та c_1 координат, що дорівнюють 1. Кожний вектор f_1 зберігається у геш-таблиці за адресами з певної множини $A(f_1)$, яка залежить тільки від вектора $\mathrm{NP}_B(\hat{f}_1)$, де $\hat{f}_1 = f_1(0_{r\times 1}, 0_{r\times(n-r)}, H_1)$, та складається з деяких двійкових векторів довжини $2n-r+1$. Множини адрес збудовані таким чином, що $A(f_1')\cap A(f_1'')\neq\varnothing$, якщо різниця між векторами $\mathrm{NP}_B(\hat{f}_1')$ та $\mathrm{NP}_B(\hat{f}_1'')$ є малим вектором.

Кожного разу, коли в процесі перебору здійснюється повторне звернення до таблиці за тією ж самою адресою, тобто для деяких векторів f_1', f_1'', що перебираються, виконується умова $A(f_1')\cap A(f_1'')\neq\varnothing$, обчислюється вектор (F_1,F_2,g), де $F_1 = f_1' + f_1''$, $(\nu,F_2,g)=\mathrm{NP}_B(\hat{f}_1')+\mathrm{NP}_B(\hat{f}_1'')$, для якого перевіряються умови (а) і (б) та рівність $\nu=1$. Отже, атака завершується успішно, якщо існує пара малих векторів f_1', f_1'', що задовольняють таким умовам:

(а′) кожний з векторів f_1', f_1'' має точно c_{-1} координат, що дорівнюють -1, та c_1 координат, що дорівнюють 1;

(б′) вектор $F_1 = f_1' + f_1''$ задовольняє умові (а);

(в′) вектор $\mathrm{NP}_B(\hat{F}_1)$ дорівнює $\mathrm{NP}_B(\hat{f}_1')+\mathrm{NP}_B(\hat{f}_1'')$, має першу координату $\nu=1$ і задовольняє умові (б).

У [16] з використанням евристичних міркувань отримано формулу для трудомісткості другого етапу описаної атаки:

$$T_2(\delta,r)=\frac{2^{15}r!}{c_{-1}!c_1!(r-c_{-1}-c_1)!}\left(\binom{2c_{-1}}{c_{-1}}\binom{2c_1}{c_1}p\,|S|\right)^{-1/2}\frac{1}{\tilde{p}}, \tag{14}$$

де

$$p=\prod_{i=1}^{2n-r+1}\left(1-\frac{1}{r_i B\left(\frac{2n-r}{2},\frac{1}{2}\right)}\int_{-r_i-1}^{-r_i}\int_{\max\{-1,z-r_i\}}^{z+r_i}(1-t^2)^{\frac{2n-r-2}{2}}dtdz\right), \tag{15}$$

$$|S|=2+2(n-t-1)p_S, \tag{16}$$

$$p_S=\frac{p_{\mathrm{NP}}2^{-4c_1}r!}{(2c_{-1})!(2c_1)!(r-2c_{-1}-2c_1)!}\binom{n-r}{4t-4c_1}\binom{n}{2t}^{-1}, \tag{17}$$

$$p_{\mathrm{NP}}=\prod_{i=1}^{2n-r+1}\left(1-\frac{2}{r_i B\left(\frac{2n-r}{2},\frac{1}{2}\right)}\int_{-1}^{\max\{-r_i,-1\}}(1-t^2)^{\frac{2n-r-2}{2}}dt\right), \tag{18}$$

$$\tilde{p}=1-(1-p_S)^{n-t}. \tag{19}$$

У формулах (15), (18) $B(\cdot,\cdot)$ позначає бета-функцію Ейлера, а числа r_i визначаються за формулами

$$r_i = \frac{R_i(\delta)}{2l},\ i \in \overline{1, 2n-r+1}, \tag{20}$$

де

$$R_i(\delta) = q,\ \text{якщо}\ 1 \le i \le 2n-r+1-\mu;$$

$$R_i(\delta) = q^{-2(i-(2n-r+1-\mu)-1)+\mu} q^{\frac{\mu-(n-r)}{\mu}},\ \text{якщо}\ 2n-r+1-\mu < i \le 2n-r+1,$$

$$\mu = \min\left\{2n-r+1, \left\lfloor \sqrt{\frac{n-r}{\log_q \delta}} \right\rfloor\right\},\ \delta > 1.$$

При цьому рекомендується використовувати такі значення параметрів:

$$|c_{-1}| = |c_1| = \left\lceil \frac{rt}{2n} \right\rceil,\ l = \sqrt{\frac{2n}{3} + \frac{2t(n-r)}{n}}. \tag{21}$$

Для оцінювання першого етапу гібридної атаки (побудови редукованого базису B решітки L) використовується традиційний підхід [18]. Вважається, що базис B будується за допомогою блокового алгоритму Коркіна – Золотарьова: BKZ 2.0 [19] (який вважається на сьогодні одним з найкращих алгоритмів розв'язання подібних задач). Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають так звані довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим базис повної решітки вимірності $2n-r+1$ за $2^{E(\beta,m,2n-r+1)}$ операцій, де

$$E(\beta, m, 2n-r+1) = 0{,}000784314\beta^2 + 0{,}366078\beta + \log((2n-r+1)m) + 0{,}875 \tag{22}$$

(зауважимо, що формула (22) є емпіричною оцінкою, яка базується на результатах обчислювальних експериментів [18]).

Мірою якості редукованого базису, який будується за допомогою алгоритму, є так званий кореневий фактор Ерміта (root Hermite facror): число $\delta > 1$, що визначається за формулою

$$\| b_1 \|_2 = \delta^{2n-r+1} \left(\det L(H_2, h)\right)^{\frac{1}{2n-r+1}} = \delta^{2n-r+1} q^{\frac{n}{2n-r+1}},$$

де b_1 є найкоротшим вектором у побудованому базисі. У [19] описано симулятор алгоритму BKZ 2.0, який дозволяє обчислювати за вхідним параметром $\delta > 1$ такі значення параметрів β і m, що застосування алгоритму BKZ 2.0 з цими параметрами до будь-якого вхідного базису повної решітки вимірності $2n-r+1$ призводить до її редукованого базису з кореневим фактором Ерміта δ.

Розрахунок трудомісткості $T_1(\delta, r)$ першого етапу гібридної атаки здійснюється наступним чином:

1) використовуючи симулятор алгоритму BKZ 2.0 [19], знайти β і m за вхідними даними $2n-r+1$ і δ;

2) покласти

$$T_1(\delta, r) = 2^{E(\beta,m,2n-r+1)}, \tag{23}$$

де $E(\beta, m, 2n-r+1)$ визначається за формулою (22).

Загальна трудомісткість гібридної атаки обчислюється за формулою

$$T(\delta, r) = T_1(\delta, r) + T_2(\delta, r); \tag{24}$$

при цьому оцінкою стійкості криптосистеми відносно цієї атаки є число $T_{\min} = \min\{T(\delta, r) : \delta > 1, r \in \overline{1, n-1}\}$.

Згідно з [16] для обчислення значення $T_{\min}$ слід для кожного $r \in \overline{1, n-1}$ знайти таке $\delta_r > 1$, що $T(\delta_r, r) = \min\{T(\delta, r) : \delta > 1\}$ та покласти $T_{\min} = \min\{T(\delta_r, r) : r \in \overline{1, n-1}\}$. Для знаходження δ_r можна застосувати ітераційний алгоритм (дихотомії), виходячи з того, що $T_1(\delta, r)$ є спадаючою, а $T_2(\delta, r)$ – зростаючою функцією параметра $\delta > 1$: шукане значення δ_r приблизно дорівнює кореню рівняння $T_1(\delta, r) = T_2(\delta, r)$.

Таким чином, використовуючи формули (14), (23), (24), можна оцінити стійкість криптосистеми, що розглядається, відносно гібридної атаки. Для забезпечення стійкості на рівні k достатньо виконання умови

$$2^k \le T_{\min}. \tag{25}$$

Методи решета

Такі атаки сьогодні реалізуються на звичайних комп'ютерах, але у майбутньому можлива їх реалізація і на квантових комп'ютерах.

Протягом останніх років запропоновано низку алгоритмів розв'язання задач SVP та CVP за допомогою методів решета. Найефективніші з відомих сьогодні таких алгоритмів мають евристичну трудомісткість $(3/2)^{N/2+o(1)}$ при $N \to \infty$, де N – вимірність решітки, причому залишковий член $o(1)$ є додатним [20, 21]. Оскільки в нашому випадку $N = 2n+1$, то для забезпечення стійкості криптосистеми відносно атак, що базуються на методах решета, достатньо виконання умови

$$2^k \le (3/2)^n. \tag{26}$$

Висновки

1. Аналіз вимог до постквантових криптоперетворень асиметричного шифрування дозволяє зробити висновок, що основною, причому безумовною вимогою щодо криптоперетворення «NTRU Prime IIT Ukraine», є вимога криптографічної стійкості щодо відомих та потенційно можливих атак. Вказані атаки можуть бути реалізовані з використанням як класичних атак на основі використання класичних комп'ютерних систем та класичних математичних методів, так і на основі квантових комп'ютерів та відповідних математичних і програмних методів.

2. Очевидно, що криптографічні асиметричні перетворення повинні забезпечувати захист як від класичних, так і від квантових методів криптоаналізу. Вказане має враховуватись, по можливості, при побудуванні та аналізі взагалі постквантових криптоперетворень, та прийнятті на їх основі постквантових стандартів асиметричних криптоперетворень.

3. У криптосистемі «NTRU Prime IIT Ukraine» в якості основного криптоперетворення, як в NTRU Prime, на відміну від NTRU, застосовується перетворення в скінченному полі. Вказане унеможливлює проведення щодо криптографічної системи «NTRU Prime IIT Ukraine» ряду потенційних атак та виключає потенційні слабкості, що присутні криптосистемі NTRU. В основному вони пов'язані з існуванням нетривіальних підкілець чи факторкілець фактор кільця (зрізаних) поліномів.

4. У криптосистемі «NTRU Prime IIT Ukraine» поліноми F та r є довільними t-малими, вони мають $2t$ ненульових коефіцієнтів (+1, -1), в той час як в NTRU кожний з зазначених поліномів має точно t ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно. Аналогічне справедливе і для полінома g, який використовується у криптосистемі «NTRU Prime IIT Ukraine», є довільним малим поліномом з $2t$ ненульових коефіцієнтів (+1, -1). Вказане дозволяє розширити у порівнянні з NTRU розмір ключового простору без втрати ефективності реалізації алгоритмів формування ключів та виконання алгоритмів зашифрування і розшифрування.

4. Для забезпечення стійкості криптосистеми відносно атаки з відомим відкритим повідомленням, яка базується на переборі векторів $b \in \{0,1\}^{l_2}$, значення l_2 (з урахуванням квантових алгоритмів перебору) повинно бути не менше ніж $2k$, де k – параметр безпеки. При цьому довжина початкового стану генератора гами, що використовується для отримання вектора b, повинна бути не менше ніж $2k+64$ біт.

5. Для криптосистеми «NTRU Prime IIT Ukraine» від найбільш ефективних з відомих потенційних атак необхідно обґрунтовано вибирати параметри n, t і q у залежності від параметра безпеки k. При цьому необхідно забезпечити виконання таких умов:

1) вибирати просте число n таким чином, щоби воно задовольняє нерівності (26);

2) для заданого n вибрати, за умови існування, натуральне t, яке задовольняє нерівності (2);

3) для заданих n та t вибрати проте число $q \geq 48t+3$ таке, щоби поліном $x^n - x - 1$ був незвідним над полем $\mathbf{Z}_q$, та виконувалась умова (25).

6. Достатньою умовою криптографічної стійкості криптоперетворення «NTRU Prime IIT Ukraine» з заданою трійкою параметрів (n,t,q) є безумовне виконання умови (25).

Список літератури: 1. *ETSI GR QSC 001 V.1.1.1 (2016-07).* Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. [Електронний ресурс]. – Режим доступу: https://portal.etsi.org/webapp/workProgram /Report_WorkItem.asp?wki_id=46690. 2. *Koblitz Neal* A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes. – Режим доступу: https://eprint.iacr.org/2015/1018.pdf. 3. *Lily Chen* Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. – Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. 4. *Mosca M.* Setting the Scene for the ETSI Quantum-safe Cryptography Workshop / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27, 2013. – Режим доступу: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/eproceedings_Crypto_2013.pdf. 5. *Post-quantum* crypto project. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html. 6. *Proposed* Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-draft-aug-2016.pdf. 7. Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges. ETSI White Paper No. 8, 2015. [Електронний ресурс]. – Режим доступу: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf. 8. *American* National Standard for Financial Services – Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry – ANSI X9.98–2010, 2010. – 284 p. 9. *Daniel J.* Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal: NTRU Prime. – Режим доступу: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf. 10. *Качко О. Г.* Оптимізація NTRU подібного алгоритму для несиметричного шифрування з "незручними параметрами" / О. Г. Качко, Л. В. Макутоніна, О. С. Акользіна // Математичне та комп'ютерне моделювання. Серія: Техн. науки, 2017. – 15 (2017). – С. 79–85. 11. *Hoffstein J.* NTRU: a ring based public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // Algorithmic Number Theory, Third International Symposium, Portland, Oregon, USA, June 21 – 25, 1998. – Proceedings. – Springer, 1998. – P. 267–288. 12. Campbell P., Groves M., Shepherd D. SOLYLOQUI: a cautionary tale, 2014. – Режим доступу: http:docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systams_and_Ayyacks/S07_Groves_Annex.pdf.
13. *Howgrave-Graham N.* A hibrid lattice-reduction and the meet-in-the-midle attack against NTRU / N. Howgrave-Graham // Advances in Cryptology – CRYPTO 2007. – Proceedings. – Springer-Verlag. – 2007. – P. 150–169. 14. *Howgrave-Graham N.* A meet-in-the-midle attack on an NTRU private key / N. Howgrave-Graham, J. H. Silverman, W. Whyte // Technical report, NTRUCryptosystems, June 2003. Report, 2003. 15. *Coppersmith D.* Lattice attack on NTRU / D. Coppersmith, A. Shamir // Advances in Cryptology – EUROCRYPT'97. – Proceedings. –

Springer-Verlag. – 1997. – P. 52–61. 16. *Wunderer Th.* Revising the hibrid attack: improved analysis and refined security estimates. – Режим доступу: http://eprint.iacr.org/2016/733. 17. *Babai L.* On Lova′sz' lattice reduction and the nearest lattice point problem / L. Babai // Combinatorica. – 1986. – Vol. 5. – № 6(11). – P. 1–13. 18. *Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z.* Choosing parameters for NTRUEncrypt. – Режим доступу: http://eprint.iacr.org/2015/708. 19. Chen Y. BKZ 2.0: better lattice security estimates / Y. Chen, P.Q. Nguyen // Advances in Cryptology – ASIACRYPT 2011. – Proceedings. – Springer-Verlag. – 2011. – P. 1–20. 20. *Горбенко Ю. І.* Спеціальна тема / Ю. І. Горбенко, Р. С. Ганзя // Зб. наук. праць, вип.2(22) Спеціальні телекомунікаційні системи та захист інформації, прим. №59 ДССЗЗІ України. – С. 17–26. 21. *Горбенко Ю. І.* Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера / Ю. І. Горбенко, Р. С. Ганзя // Захист інформації. – 2014. – Т. 16, №2. – С. 106–112. 22. *Горбенко Ю. І.* Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко, Р. С. Ганзя // Вісник Нац. ун-ту «Львівська Політехніка». Сер. «Комп'ютерні системи та мережі», 2014. – № 806. – С. 40–49. 23. *J. Silverman and A. Odlyzko*. NTRU Report 004, Version 2, A Meet-The Middle Attack on an NTRU Private Key, Technical Report, NTRU Cryptosysytems, (2003). 24. *A Chosen-Ciphertext* Attack against NTRU. [Електронний ресурс]. – Режим доступу: http://www.iacr.org/archive/crypto2000/18800021/18800021.pdf. 25. *Information* technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms : ISO/IEC 9796-2:2010. – 54 p. 26. *IBM* Raises the Bar with a 50-Qubit Quantum Computer. [Електронний ресурс]. – Режим доступу: https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/?utm_campaign=add_this&utm_source=twitter&utm_medium=post. 27. *Создан* первый квантовый компьютер на 53 кубитах. [Електронний ресурс]. – Режим доступу: https://hightech.fm/2017/11/30/53-qubit.

Акціонерне товариство
«Інститут інформаційних технологій»,
Харківський національний
університет радіоелектроніки,
Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 06.10.2017

УДК 004.056.55

Ю.І. ГОРБЕНКО, канд. техн. наук, К.В. ІСІРОВА

УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ

Вступ

Розробка та стандартизація постквантових асиметричних криптографічних перетворень є однією із важливих проблем сучасності. Провідні держави, в тому числі США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів електронного підпису(ЕП) та асиметричного направленого шифрування (НШ), які будуть актуальними та можуть застосовуватись у постквантовий період, оголосив конкурс на розробку стандартів постквантових асиметричних криптографічних примітивів [1 – 3]. Заявки приймались NIST до 30 листопада 2017 року. Вони стосуються в першу чергу асиметричних алгоритмів ЕП. Європейський Союз (ЄС) також веде активну роботу з розробки та досліджень постквантових стандартів асиметричних криптографічних перетворень , в тому числі стандартів постквантового ЕП. Вказане пояснюється їх широким застосуванням в значному числі додатків та можливими великими втратами у випадку компрометації ЕП, коли з'явиться квантовий комп'ютер з необхідними характеристиками та можливостями [1 – 5].

Дослідження, проведені в технологічно розвинутих державах, показали, що одним із перспективних напрямів створення постквантового ЕП, може бути напрям, що ґрунтується на використанні функцій гешування та дерева Мерклі [6]. В основу цього напряму покладено використання одноразових ключів та одноразових ЕП. На нинішній час запропоновані та суттєво досліджені такі механізми генерування та використання одноразових ключів ЕП на основі функцій гешування (симетричних криптографічних перетворень та функцій зчеплення):

- механізм Лампорта з одноразовими ключами LOTS [7];
- механізми Вінтерніц з одноразовими ключами *WOTS*, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 10];
- модифікації механізму з одноразовими ключами Biba, HORS, HORS+, HORS++ та HORST [10].

Нами запропоновано удосконалений механізм з одноразовими ключами, що названий POTS [13]. Мета статті – обґрунтування необхідності, детальне викладення сутності, дослідження властивостей за критеріями складність – криптографічна стійкість, визначення переваг та недоліків, а також умов і можливостей застосування удосконаленого механізму POTS в різних додатках постквантового періоду.

1. Постановка проблеми та можливості її вирішення

Суттєвим розвитком механізму ЕП на основі *OTS є* механізм Вінтерніц [4, 8]. Хоча механізми OTS Лампорта та LD-OTS Лампорта – Діффі забезпечують потенційні можливі властивості криптографічної стійкості ЕП, а по суті – зашифрування), але розміри ЕП та OTS ключів залишаються досить великими. Зменшення розміру ЕП досягається в механізмі одноразового ЕП з OTS, що запропонована в [4, 13], який отримав назву механізму Вінтерніц (W OTS) [8]. Ідея механізму Вінтерніц полягає в тому, щоб підписувати, на відміну від OTS Лампорта, уже декілька бітів геш-значення, використовуючи одну послідовність OTS секретного одноразового ключа. Іншою особливістю механізму Вінтерніц є застосування одно направлених фунцій, які, на наш погляд, можна назвати функціями зчеплення. Особливістю застосування функцій зчеплення є можливість виділення відкритого ключа безпосередньо із отриманого ЕП. На наш погляд, це є принциповою особливістю механізму Вінтерніц. Але, в цій статі ми будемо ставити механізм Вінтерніц в одинакові умови з механізмом Вінтерніц.

Як в механізмах OTS Лампорта та Лампорта – Діффі, в механізмі Вінтерніц (WOTS) використовуються одностороння геш-функція та криптографічна геш-функція. Параметр Вінтерніц ЕП $w \geq 2$ обирається як кількість бітів, що повинні бути підписані (зашифровані) одночасно з використанням одноразового ключа. Запропоновано також варіант ЕП Вінтерніц WOTS з використанням додаткового методу контролю цілісності на основі контрольної суми геш-значення, що зашифровується. Застосування додаткового методу контролю цілісності має на меті підсилення стійкості ЕП Вінтерніц WOTS.

Також аналіз показав, що у основних роботах, що стосуються одноразових ключів, в недостатній мірі використовуються «істинно» криптографічні критерії оцінки криптографічної стійкості та складності. На наш погляд, при оцінці та порівнянні різних механізмів ЕП з OTS, необхідно, як мінімум, використовувати [5]:

- Lc, Lв та Lп – відповідно довжини секретних Кс та відкритих ключів Кв та відкритого ЕП;

- число секретних Nк одноразових ЕП WOTS ключа, що можуть бути використані з рівною ймовірністю;

- ентропія джерела ключів H(Nк) відповідної модифікації одноразового ЕП WOTS ключа;

- безпечний час $T_б$ у вигляді математичного сподівання часу розкриття криптографічної системи при застосуванні відомих силових та аналітичних атак за допомогою як класичних та і квантових комп'ютерів, в нашому випадку наприклад визначення секретного ключа за умови ЕП та як наслідок одноразовому відкритого ключа ЕП OTS ;

- відстань єдності джерела l_0 одноразових OTS секретних ключів ЕП ;

- складність здійснення успішного криптоаналізу *Іс ЕП з OTS* при застосуванні силових методів;

- складність здійснення успішного криптоаналізу *Іа ЕП OTS* при застосуванні аналітичних методів.

Основні визначення та порядок застосування запропонованих критеріїв та показників оцінки *ЕП* на основі *OTS* повинні застосовуватись в необхідній при аналізі та порівнянні.

Проведений аналіз основних механізмів з одноразовими ключами – OTS Лампорта, OTS Вінтерніц (*WOTS*, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 9]) та модифікації механізму з одноразовими ключами (Biba, HORS, HORS+, HORS++ та HORST[ ]) не задовольняють вимогам просторової та часової складності, що суттєво ускладнює реалізацію постквантових ЕП на основі функцій гешування. Справа в тому, що при спробах зменшити розміри ключів та ЕП, робиться відхід від істинно бездоганних ЕП [13 – 15]. В той же час, на наш погляд, існує можливість побудування постквантових ЕП на основі OTS ключів, у вигляді perfekt OTS (POTS) [13], які за властивостями практично не уступали механізму Лампорта. Тому розглянемо *сутність, результати дослідження властивостей, переваги та недоліків, а також умови і можливостей застосування удосконаленого механізму* POTS *в різних додатках постквантового періоду*.

2. Удосконалена математична модель механізму постквантового ЕП POTS

Загальні положення. В Вінтерніц OTS (WOTS) механізмі ЕП існує, у порівнянні з механізмом Лампорта, можливість виробляти коротші ЕП, але число секретних та відкритих ключів зі збільшенням параметра *w* зростає суттєво. Також у загальному випадку механізму WOTS, що адекватний щодо властивостей механізму Лампорта, суттєво збільшується часова та просторова складності. Вказане обмежує застосування механізмів Вінтерніц (*WOTS,* $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 9]) для випадку, коли мають бути виконаними вимоги, аналогічні, що виконуються механізмом Лампорта. Також немає можливості використовувати секретний ключ одночасно для підпису декількох та значно більшого числа геш-значення (WFTS) [9.]. Використовуючи цю ідею, розглянемо удосконалений механізму POTS з одноразовими ключами, основними перевагами якого є можливість зменшення

довжин одноразових ключів (секретних та відкритих ключів), а також довжини ЕП. Існують також варіанти його застосування і для WFTS.

Як і в механізмах LOTS Лампорта та Лампорта – Діффі LDOTS, в удосконаленому механізмі POTS будемо використовувати односторонню чи криптографічну геш-функцію

$$f: \{0, 1\}1 \rightarrow \{0, 1\}^{1} \tag{1}$$

та обов'язково криптографічну геш-функцію

$$g: \{0, 1\}* \rightarrow \{0, 1\}^{1.}$$

При ЕП повідомлення M спочатку здійснюється гешування повідомлення M з використанням узгодженої (як правило криптографічної) геш-функції з параметрами Pr та обчислюється геш-значення

$$h_M = H(M, Pr)) \tag{2}$$

Далі значення h_M зашифровується засобом заміни w блоків бітів геш-значення h_M секретними одноразовими ключами Процес такого зашифрування продовжується для усіх блоків бітів геш-значення h_{Mi}.

Таким чином, l_h бітів геш-значення h_{Mi} заміняються (зашифровуються) одноразовими ключами, по суті безумовно стійким шифром, оскільки послідовність бітів h_{Mi} заміняється одноразовими секретними випадковими послідовностями. Вказана послідовність l_k секретних послідовностей і є ЕП повідомлення *M*. Такий ЕП разом з вибраними із x_i чи y_i послідовностями стає відкритим та доступним як користувачам (перевірникам) відповідного домену, так і порушнику (криптоаналітику). В подальшому такий ЕП у відповідному форматі передається та зберігається разом з повідомленням і є його одноразовим ЕП. У випадку механізму POTS ЕП складається з *k випадкових послідовностей, причому* $k \le l_h$.

Генерація ключів для механізму POTS. Будемо вважати, що параметр w ≥ 1 визначає кількість бітів геш-значення, що повинна бути підписана одночасно, тобто замінена одним секретним ключем. Причому, при w=1 маємо частковий випадок – механізм Лампорта з OTS ключами. При w ≥ 2 маємо загальне подання механізму Вінтерніц, хоча в подальшому функція зашифрування та перевірки буде модифікуватись.

В механізмі POTS ЕП (зашифрування) здійснюється (не обов'язково) на основі застосування до усіх w_b блоків перетворення виду

$$z = Z(w_b), \tag{3}$$

внаслідок чого *w* біт блоку відображаються в *w** біт нового блоку. Причому L_{bi} довжина b_i блоку може бути як більше, так і менше довжини L_{bi^*} блоку b_i^*, отриманого внаслідок перетворення (3).

Зразу відмітимо, що головною відмінністю механізму POTS є те, що в ньому застосовується перетворення кожного b_i блоку згідно [13] у такому вигляді. Якщо

$$0 \le b_i \le (2^w / 2) - 1 \tag{4}$$

то кожен b_i блок зашифровується (заміняється) послідовно секретним ключем із множини X, інакше зашифровується (заміняється) послідовно секретним ключем із множини Y.

По аналогії з узагальненням Вінтерніц визначимо параметри t_1, t_2, t у вигляді [7, 8]

$$t_1 = \left\lceil l / \log_2 w^* \right\rceil, t_2 = \left\lceil \log_2 t_1((w^* - 1)) / \log_2 w^* \right\rceil + 1, t = t_1 + t_2 . \quad (5)$$

Будемо вважати, що для геш-значення повідомлення, що подається у вигляді блоків b_i (b_i^*) виду

$$\mathrm{d} = \mathrm{bt1\text{-}1} \,||\, .\mathrm{bi} \,.\,.\, ||\, \mathrm{b0}\ , \quad (6)$$

можна визначити контрольну суму у вигляді [7]

$$c^* = \sum_{i=1}^{t_1} (w^* - 1 - b_i^*) \quad (7)$$

чи у вигляді

$$c^* = \sum_{i=1}^{t_1 1} (2^{w^*} - b_i^*)\ , \quad (8)$$

тощо.

В моделі POTS не виключається, що параметри t_1, t_2, t можуть бути визначеними іншим чином. В механізмах POTS дані геш-значення d (6) та контрольних сум *C* (7) та (8) можуть зашифровуватись з різною збитковістю, наприклад для контрольної суми з більшою чи меншою у залежності від вимог збитковістю.

Разом з тим, попередній аналіз показав, що вид функцій перетворення блоків (3) та (4) може суттєво вплинути на криптографічну стійкість проти існуючих та можливих атак. Тому, однією із важливих задач цього дослідження, є визначення функцій перетворення, які будуть дозволяти забезпечити зменшення довжин секретних та відкритих ключів, а також зменшувати довжину ЕП, забезпечуючи допустиму криптографічну стійкість проти існуючих та потенційних атак на основі класичних та квантових комп'ютерів.

Після виконаного перетворення (6) чи (7) значення контрольної суми C^* у вигляді блоків бітів w^* конкатенується з геш-значенням (6) *d* і потім виконується одночасне ідентичне зашифруваннння POTS та верифікація. Відмітимо, що контрольні суми можуть обчислюватись довільним чином у залежності від необхідності. Крім того, значення ЕП d та контрольних сум C (7) та (8) тощо, можуть зашифровуватись згідно OTS.

Уточнення параметрів для POTS. Для здійснення ЕП спочатку уточнимо параметри підпису – *t*1, *t*2 та *t*. Якщо довжини L_s випадкових чи псевдовипадкових послідовностей кратні w^*, то *t*1 визначає кількість блоків бітів геш-значення, що будуть підписуватись (зашифровуватись) одним секретним ключем. В цьому випадку

$$t = t1 = n / w^* \quad (9)$$

Якщо *n* не кратне w^* , то в останньому блоці буде менше чим w^* бітів, тому число бітів, які потрібно підписати необхідно збільшити так, щоб t_1 було цілим. В (8) *t*2 визначає число блоків, за допомогою яких подається контрольна сума. У загальному випадку

$$t^* = t1 + t2 \quad (10)$$

Без втрати як теоретичного так і практичного подання та дослідження WOTS можна (але не обов'язково) вважати, що довжина блока w = 1,2,3,3.,4.6…., за цієї умови для однозначного зашифрування кожного із w_i блоків потрібно у загальному випадку

$$N_w = 2^w,\ w = 2,3,4,5,6... \quad (11)$$

випадкових послідовностей кожного секретного ключа.

У випадку (4) для зашифрування кожного w_i блоку необхідно

$$N_w = 2 \tag{12}$$

випадкових послідовностей кожного секретного ключа. Тому, у залежності від значення w, виграш U у зменшенні довжини секретного ключа у загальному випадку для POST стосовно WOST складає

$$U = 2^{w-1}. \tag{13}$$

Секретним ключем ЕП POTS $X_d\ (w^*), Y_d\ (w^*)$ є послідовність t множин секретних ключів

$$\begin{aligned} X_d(w^*) &= (x_{t-1},\ldots,\ x_i,\ \ldots,\ x_0) \\ Y_d(W^*) &= (y_{t-1},\ldots,\ yi,\ \ldots,\ y_0) \end{aligned} \tag{14}$$

з довжиною кожної із секретних послідовностей $l(w^*)$.

Кожна множина (14) секретних ключів $X_d\ (w^*), Y_d\ (w^*)$ є частиною секретного (особистого) ключа.

Відкритий ключ перевірки ЕП для механізму POTS обчислюється засобом гешування секретних ключів (14) з застосуванням одно направленої чи криптографічної геш-функції f (g). Внаслідок отримуємо t множин по 2 відкритих ключів в кожній:

$$\begin{aligned} H_d(X) &= H(x_{t-1}),\ldots,\ \mathrm{H}(x_i),\ \ldots,\ \mathrm{H}(x_0) \\ H_d(Y) &= H(y_{t-1}),\ldots,\ \mathrm{H}(y_i),\ \ldots,\ \mathrm{H}(y_0) \end{aligned} \tag{15}$$

з довжиною геш-значення l_h кожної послідовності секретного ключа.

Вироблення ЕП для механізму POTS.

Нехай повідомлення M має геш-значення

$$g(M) = h = (h_l,\ldots,h_i,\ldots,h_0), \tag{16}$$

яке потрібно підписати з використанням криптографічної геш-функції g.

У загальному випадку, якщо l_h не кратне w^*, то до l_h додається необхідне число нулів, так щоби довжина l_h була кратна w^*. Рядок l_h бітів розділяється на t блоків $b_{t-1},\ldots,b_i,\ldots,b_0$ з довжиною w бітів кожен. Але ми будемо розглядати, як правило, не втрачаючи загальність випадок (9).

В подальшому для ЕП та перевірки ЕП будемо застосовувати правила, коли довжина блока буде змінюватись. В результаті такого перетворення w біт b_i блоку відображаються в w* біт b_i^* нового блоку, а довжина L_{hi^*} нового блоку b_i^* може бути як більше, так і менше довжини L_{hi} блоку b_i, отриманого внаслідок перетворення (7).

Таким чином, в механізмі POTS здійснюються такі попередні перетворення:

- рядок l_h бітів геш-значення розділяється на t блоків $b_{t-1},\ldots,b_i,\ldots,b_0$ з довжиною w бітів кожного блоку;

- w біт b_i блоків відображаються в w* біт нових b_i* блоків, причому діючим випадок, коли $b_i* = b_i$;

- w* біт нових блоків (3) b_i* зашифровуються з використанням секретного ключа ($X_d\ (b_i*), Y_d\ (b_i*)$) згідно (12) – (14) з довжиною кожної із секретних послідовностей $l(w^*)$.

Таким чином, на відміну від механізму Вінтерніц, в механізмі POTS w біт b_i блоків відображаються в w^* біт b_i^* блоків, які можуть мати як меншу довжину, так і більшу по відношенню до w .

В результаті ЕП має такий вигляд

$$\{M; Z^* = (\{x_{t^*-1} \mid y_{t^*-1}\}), \{x_{t^*-2} \mid y_{t^*-2}\}, ..., \{x_i \mid y_i\}, ..., \{x_0 \mid y_0\}) =$$

$$\{M, Z^* = (z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)\} \tag{17}$$

В (17) символ « | » означає, що при зашифруванні в ЕП з'являється одна із використаних секретних послідовностей – x_i чи y_i, що визначається i-м блоком довжини w* бітів. В подальшому параметр t^* означає число блоків, яке може бути як більше, так і менше t, а також дорівнювати t.

Перевірка ЕП для механізму POTS. Перевірка ЕП здійснюється у такій послідовності.

1) Із використанням криптографічної геш-функції g здійснюється гешування повідомлення M^*, для якого робиться перевірка ЕП, в результаті отримується геш-значення

$$h_{Mi^*} = g(M^*, \Pr). \tag{18}$$

Якщо довжина h_{Mi^*} не кратна w, то до рядка бітів h_{Mi^*} у відповідності з домовленістю добавляється деяке число нулів, так щоб довжина h_{Mi^*} була кратна w. Рядок h_{Mi^*} бітів розділяється на t* блоків $b_{t^*-1}, ..., b_i, ..., b$ 0 довжини w* бітів кожний.

2) У відповідності зі значеннями b_i блоків h_{Mi^*} із відкритого ключа перевірки ЕП (15) вибираються геш-значення $H(x_i)$ чи $H(y_i)$, внаслідок отримуємо, що

$$Z^* = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\}, ..., \{H(x_i) \mid H(y_i)\}, ..., \{H(x_n) \mid H(y_n)\}) =$$

$$= (z^*_{t-1}, z^*_{t-2}, ..., z^*_i, ..., z^*_0) \tag{19}$$

3) Наостанок користувач, що отримав підписане повідомлення, гешує усі послідовності ЕП (17), отримує їх геш-значення

$$(H(z_{t^*}), H(z_{t^*-1}), ..., H(z_i), ..., H(z_0)) \tag{20}$$

та порівнює отримані значення зі значеннями (17), тобто $(z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)$. Якщо усі t^* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим.

3. Дослідження складності ЕП з OTS ключами на основі геш-функцій

В цьому параграфі розглянемо можливі алгоритми (механізми) реалізації (3), орієнтуючись на їх нелінійність, та як внаслідок можливості зменшення довжин ключів та довжин ЕП з однозначним визначенням криптографічної стійкості проти атак на основі класичних та квантових комп'ютерів. Будемо вважати, що секретним ключем POTS є множина секретних випадкових послідовностей у відповідності з (14). Відкритим ключем ЕП Y є послідовність рядків, що обчислюється шляхом гешування множини секретних випадкових послідовностей з використанням геш-функції f ь (15).

Далі в механізмі POTS зашифрування здійснюється на основі застосування до b_i блоків перетворення виду

$$b_i^* = Z(b_i) \ , \tag{21}$$

внаслідок чого w біт b_i блоку відображаються в w^* біт нового b_i^* блоку. Довжина b_i^* блоку w^*може бути рівною w, більшою чи меншою за w.

На наступному етапі здійснюється ЕП (зашифрування) з використанням механізму POTS (17) та [13]. Внаслідок маємо, що

$$Y=(y_{t^*-1},\ldots,y_i,\ldots,y_1,y_0)\in\{0,1\}^{(l,\ t\times 2)} \tag{22}$$

де

$$y_i=f(b_i^*),0\le i\le(l,2\times t-1. \tag{23}$$

Далі з використанням POTS механізму здійснюється ЕП.

Будемо вважати, що підписане повідомлення має такий вигляд

$$\{M;Z=(\{x_{t^*-1}\mid y_{t^*-1}\}),\{x_{t^*-2}\mid y_{t^*-2}\},\ldots,\{x_i\mid y_i\},\ldots,\{x_0\mid y_0\})=$$
$$=\{M,Z=(z_{t^*},z_{t^*-1},\ldots,z_i,\ldots,z_0)\} \tag{24}$$

В (24) символ « | » означає, що при зашифруванні в ЕП появляється одна із використаних секретних послідовностей x_i чи y_i, що визначається *i-м* блоком бітів довжини w*.

За умов (21) – (23) число секретних та відкритих послідовностей ключів, а також довжина ЕП можуть як скорочуватись, так і розширюватись. Детально розглянемо це нижче.

Перевірка ЕП для механізму POTS. Перевірка ЕП здійснюється у такій послідовності.

1) Із використанням криптографічної геш-функції g здійснюється хешування повідомлення M^*, для якого робиться перевірка ЕП, в результаті отримується геш-значення $h_{Mi^*}=H(M^*,\Pr)h_{Mi}$.

2) Якщо довжина h_{Mi^*} не кратна w, то до рядка бітів h_{Mi^*} у відповідності з домовленістю добавляється деяке число нулів так, щоб довжина h_{Mi^*} була кратна w. Рядок h_{Mi^*} бітів розділяється на t^* блоків $b_{t-1},\ldots,b_i,\ldots,b_0$ довжини w бітів кожний.

3) Кожний b_i блок довжини w згідно (19) перетворюється в w^* біт нового b_i^* блоку.

4) У відповідності зі значеннями b_i^* блоків геш-значення із відкритого ключа перевірки ЕП вибираються геш-значення $H(x_i)$ чи $H(y_i)$. Внаслідок отримуємо

$$Z^*=(\{H(x_1)\mid H(y_1)\}),\{H(x_2)\mid H(y_2)\},\ldots,\{H(x_i)\mid H(y_i)\},\ldots,\{H(x_n)\mid H(y_n)\})=$$
$$=(z^*_{t^*-1},z^*_{t^*-2},\ldots,z^*_i,\ldots,z^*_0) \tag{25}$$

5) Наостанок користувач-перевірник послідовно гешує усі послідовності ЕП (24), отримує значення

$$(H(z_t),H(z_{t-1}),\ldots,H(z_i),\ldots,H(z_0)) \tag{26}$$

та порівнює отримані значення зі значеннями (25), тобто $(z^*_{t^*-1},z^*_{t^*-2},\ldots,z^*_i,\ldots,z^*_0)$. Якщо усі t^* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим.

6) Якщо в механізмах POTS чи PFTS використовується перевірка за допомогою контрольних сум C (7) чи (8), то пункти 2) – 5) виконуються і для контрольних сум c^*. При цьому, якщо зашифровування d та c здійснюється з різною збитковістю, то це враховується при перевірці ЕП.

Розглянемо та проведемо дослідження названих вище модифікацій POTS механізмів стосовно довжин секретних та відкритих ключів та довжин ЕП.

В табл. 1 наведено значення розмірів секретних l_s та відкритих ключів l_o, а також ЕП l_{sg} модифікацій OTS (LOTS, LDOTS, WOTS, P*O*TS), що отримані на основі даних, які наведені вище, у залежності від довжини блоку w. Причому прийнято, що механізм WOTS реалізовано засобом зашифрування кожного блоку w – 2^w випадковими послідовностями.

Таблиця 1

Значення розмірів секретних, відкритих ключів та ЕП модифікацій OTS (біт)

W\P$_{НАВ}$	1	2	3	8	16	32	63.	128	256
L OTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	–	–	–	–	–	–	–	–
LDOTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	–	–	–	–	–	–	–	–
WOTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	2^{17} 2^{17} 2^{15}	2^{18} 2^{18} 2^{14}	2^{21} 2^{21} 2^{13}	2^{28} 2^{28} 2^{12}	2^{43} 2^{43} 2^{11}	2^{74} 2^{74} 2^{10}	2^{138} 2^{138} 2^{9}	2^{265} 2^{265} 2^{8}
P OTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	2^{16} 2^{16} 2^{15}	2^{15} 2^{15} 2^{14}	2^{14} 2^{14} 2^{13}	2^{13} 2^{13} 2^{12}	2^{12} 2^{12} 2^{11}	2^{11} 2^{11} 2^{10}	2^{10} 2^{10} 2^{9}	2^{9} 2^{9} 2^{8}

Аналіз наведених результатів та даних табл. 1 дозволяє зробити такі висновки.

Твердження 1.

1) Розміри секретних та відкритих ключів, а також ЕП модифікацій LOTS та LDOTS співпадають. Тому такі системи OTS можна віднести до одного класу з практично однаковими властивостями.

2) При l_h =256 розміри секретних та відкритих ключів в системах LOTS та LDOTS складають відповідно 131072 бітів, а розмір ЕП 65536 бітів, тобто є суттєвими.

3) При l_h =256 та w =1 розміри секретних та відкритих ключів в усіх модифікаціях OTS, а також розмір ЕП співпадають, тобто усі модифікації OTS для цих умов по суті зводяться до LOTS.

4) В механізмі WOTS ЕП при збільшенні параметру Вінтерніц w довжини секретного та відкритого ключів скоріше всього можуть бути реалізовані при значеннях параметра Вінтерніц $w \le 8$ (див. табл. 1).

5) При застосуванні POTS механізму появляється можливість суттєво зменшити довжини як ключів так і ЕП (див. табл. 1).

6) Щодо механізму POTS необхідно додатково провести дослідження, що стосуються захищеності від атак на основі нав'язування у вигляді ЕП випадкових послідовностей, то вони наводяться нижче.

4. Дослідження захищеності POTS від нав'язування хибних ЕП

На наш погляд, усі наведені OTS механізми, особливо POTS, вимагають досліджень в частині імітостійкості та криптографічної стійкості. При цьому імітостійкість будемо розглядати у вигляді захищеності від нав'язування порушником (криптоаналітиком) хибних підписаних повідомлень.

У зв'язку з вказаним спочатку розглянемо загальний випадок перетворення значень кожного блоку b_i^* (c_i*) згідно з (23) довжиною W* на $\varepsilon*$ значень при формальних значеннях $w*, t*, \varepsilon*, l*$ в механізмі POTS. Будемо вважати, що $l*$ кратне $w*$, тому $t* = l*/w*$. Далі, кожен b_{ij}^* ($c_{ij}*$) блок ділиться на $\varepsilon*$ непозиційних підблоків. Довжина кожного підблоку $\tau = w*/\varepsilon*$.

Подальші дослідження присвячено аналізу властивостей та можливостей застосування функцій (22) та ((23).

Твердження 2. Нехай для ЕП та перевірки ЕП в механізмі POTS застосовується перетворення кожного b_i блоку згідно (4) у такому вигляді. Якщо

$$0 \le b_i \le (2^w / 2) - 1 \tag{27}$$

то b_i блок зашифровується (заміняється) послідовно секретним ключем із множини (14) X, інакше зашифровується (заміняється) послідовно секретним ключем із множини (14) Y.

Необхідно відмітити, що правило найбільш швидко може бути реалізоване засобом аналізу старшого біту, тобто 2^w. Якщо він має значення «1», то заміняється секретним ключем із множини (13) Y, інакше зашифровується (заміняється) послідовно секретним ключем із множини (14) X.

Нехай порушник робить спроби нав'язати хибне чи викривлене повідомлення $M*$, у якого хибним ЕП є l/w випадкових послідовностей. Тоді складність здійснення такої атаки визначається як

$$P_y = 2^{-t}, \tag{28}$$

де t – довжина ЕП POTS, тобто визначається кількістю випадкових послідовностей, що використані при формуванні відкритого ЕП.

Далі, якщо в (26) поділ кожного блоку здійснюється на ε інтервалів, тоді складність здійснення атаки визначається як

$$P_y = 2^{-\varepsilon t}, \tag{29}$$

Спочатку розглянемо доведення для випадку ε=2. В цьому випадку зашифрування здійснюється згідно з (26), тобто блок ділиться на дві частини і якщо виконується умова (26), то із множини секретних послідовностей (14) вибирається X відповідна послідовність, інакше із множини (14) Y послідовність з відповідним номером. Оскільки геш-значення h_{Mi} є випадковою послідовністю, то будемо вважати, що ймовірності подій (26) є рівноймовірними і для $\varepsilon = 2$ отримуємо, що для одного блоку $P_y = 2^{-1}$. Далі, за умови рівноймовірності появи блоків для t блоків отримуємо, що $P_y = 2^{-t}$.

Таким чином, доведення стійкості щодо POTS проти атаки у вигляді випадкових послідовностей ґрунтується на тому, що хибне повідомлення з ймовірністю 0.5 попадає в інтервали (26).

В табл. 2 наведено значення ймовірностей здійснення атаки на основі нав'язування хибних випадкових послідовностей у залежності від числа блоків t на основі геш-значення g при *lg =256 біт для механізму* POTS (3-я строчка).

Розглянемо також підхід до оцінки імітостійкості і для інших механізмів – LOTS, LDOTS та WOTS. Будемо вважати, що секретні ключі генеруються на основі випадкових чи псевдовипадкових процесів (генераторів). Тому за умови (26) кожен біт секретного ключа для механізмів LOTS, LDOTS може нав'язуватись (підроблятись) з ймовірністю 2^{-1}. У цілому при довжині секретного ключа l_s бітів отримаємо, що ймовірність успішного нав'язування засобом створення випадкової послідовності секретних ключів, можна оцінити як

$$P_{нав} = 2^{-ls} \tag{30}$$

Іншими методом нав'язування може бути спочатку розкриття ключа, тобто проведення успішного криптоаналізу секретного ключа. При цьому розкриття секретного ключа для вказаних механізмів може бути зроблено засобом обернення відкритих ключів, яке зводиться до знаходження прообразу геш-значень секретних послідовностей секретного ключа (випадкових послідовностей) на основі відкритого ключа. Якщо вважати, що обернення здійснюється методом створення колізії, то в даному випадку визначення секретного ключа на квантовому комп'ютерові може здійснюватись на основі методу Гровера [13, 15], а на класичноу – методом створення колізії з використанням методів Полларда [15, 16]. В даному випадку ймовірність *Pc* визначення секретного ключа після модифікації перехопленого, причому

$$Pc = 2^{-ls/2}. \tag{31}$$

Але необхідно відмітити, що (31) може бути застосовано, якщо секретний ключ використовується більше ніж один раз. Для випадку застосування одноразових ключів атакувати одноразовий OTS немає сенсу, так як він не може бути в подальшому застосований.

Іншим, на наш погляд, продуктивним методом нав'язування хибного повідомлення методом модифікації ЕП є застосування методу Гровера засобом модифікації, як мінімум половини бітів секретного ключа.

В табл. 2 наведено оцінки ймовірносне нав'язування на основі застосування при нав'язуванні хибного ЕП прямим методом (співвідношення (30)) та модифікації половини l_s бітів секретного ключа з використанням (29).

Таблиця 2

Ймовірності нав'язування хибного підпису повідомлення при *lg* =256 біт

W\P$_{НАВ}$	1	2	3.	8	16	32	63	128
L OTS	$2^{-131072}$ / $10^{-3.9*10^4}$	–	–	–	–	–	–	–
LDOTS	$2^{-131072}$ / $10^{-3.9*10^4}$	–	–	–	–	–	–	–
POTS	–	2^{-128} / $10^{-38.53}$	2^{-64} / $10^{-19.26}$	2^{-32} / $10^{-9.63}$	2^{-16} / $10^{-4.82}$	2^{-8} / $10^{-2.41}$	2^{-2} / $10^{-1.20}$	2^{-1} / $10^{-0.6}$
WOTS	$2^{-131072}$ / $10^{-3.9*10^4}$	$2^{-131072}$ / $10^{-3.9*10^4}$	$2^{-262144}$ / $10^{-7.9*10^4}$	$2^{-524288}$ / $10^{-1.6*10^5}$	$2^{-6.7*10^7}$ / 10^{-2*10^7}	$2^{-8.8*10^{12}}$ / $10^{-2.6*10^{12}}$	$2^{-1.5*10^{73}}$ / $10^{-4.5*10^{72}}$	

Визначимо значення розмірів секретного та відкритого ключів та розміри ЕП для таких значень перетворень (21) та (24) $w = 8$; w^*=2, 3.,8,1; $l_h^* = 512, 128, 256$ біт.

Причому на першому кроці з використанням криптографічної геш-функції обчислюється геш-значення $h(M)$ з довжиною $l_h = 256$ біт, потім здійснюється нелінійне перетворення отриманого геш-значення в $l_h^* = 512$ чи $l_h^* = 128$ чи $l_h^* = 256$ бітів. Нелінійність досягається на основі гешування попереднього геш-значення з розширенням 256 біт в $l_h^* = 512$ біт,чи стягуванні в $l_h^* = 128$, а також відображенні $l_h = 256$ в $l_h^* = 256$ біт. Символ (*), що використаний вище, позначає довжину геш-значення, що зашифровується.

На другому кроці отримані геш-значення діляться на блоки $w = 8$ бітів, потім діляться на підблоки довжини w^*=2, 3.,8 біт. На завершення отримані значення w* зашифровуються згідно (20-233.19) з використанням випадкових послідовностей довжини відповідно $lp = 512,128,256$ біт тощо з використанням PW OTS ключів.

Твердження 3. Параметри l_s, l_o та l_{sg} P OTS з урахуванням тверджень 1 та 2 можна визначити з використанням таких співвідношень.

Довжина секретного ключа, тобто сумарна довжина усіх випадкових послідовностей,

$$l_s = (l_h^*/8) \times 2w^* \times l_p . \tag{32}$$

Довжина відкритого ключа, тобто сумарна довжина усіх геш-значень випадкових послідовностей,

$$l_o = l_s = (l_h^*/8) \times 2w^* \times l_p . \tag{33}$$

Довжина ЕП, тобто сумарна довжина секретних ключів, що використані для ЕП,

$$l_{sg} = (l_h^*/8) \times w^* \times l_p . \tag{34}$$

В табл. 3 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h^* = 512$ біт.

Таблиця 3

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h^* = 512$ біт

$l_p \setminus w^*$	512	128	256
2	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
3	2^{18} 2^{18} 2^{17}	2^{16} 2^{16} 2^{15}	2^{17} 2^{17} 2^{16}
8	2^{19} 2^{19} 2^{18}	2^{17} 2^{17} 2^{16}	2^{18} 2^{18} 2^{17}
1	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}

В табл. 4 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$ = 128 біт.

Таблиця 4

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$=128 біт

$l_p \setminus w^*$	512	128	256
2	2^{15} 2^{15} 2^{14}	2^{13} 2^{13} 2^{12}	2^{14} 2^{14} 2^{13}
3.	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}
8	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
1	2^{14} 2^{14} 2^{13}	2^{12} 2^{12} 2^{11}	2^{13} 2^{13} 2^{12}

В табл. 5 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$ = 256 біт.

Таблиця 5

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$= 256 біт

$l_p \setminus w^*$	512	128	256
2	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}
3.	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
8	2^{18} 2^{18} 2^{17}	2^{16} 2^{16} 2^{15}	2^{17} 2^{17} 2^{16}
1	2^{15} 2^{15} 2^{14}	2^{13} 2^{13} 2^{12}	2^{14} 2^{14} 2^{13}

Для порівняння в табл. 6 наведено розміри секретних та відкритих OTS ключів та розміри ЕП для механізмів Лампорта та Лампорта – Діффі.

Таблиця 6

Розміри секретних та відкритих одноразових ключів
та розміри ЕП для механізмів Лампорта та Лампорта – Діффі

Розміри даних\ lh, n			Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	256		2^{17}	2^{17}	2^{16}
512	512		2^{19}	2^{19}	2^{18}

В табл. 7 наведено результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізму Вінтерніц. Довжина секретного та відкритого ключів визначається як $2 \times w^2 \times n_i \times l_h$, довжина ЕП $n_i \times l_h$

Таблиця 7

Результати оцінки розмірів секретних та відкритих одноразових ключів
та розмірів ЕП для механізму Вінтерніц

Розміри даних\lh, n_i	w_i		Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
2256	128	2	2^{18}	2^{18}	2^{15}
	63	3.	2^{19}	2^{19}	2^{14}
	32	8	2^{23}	2^{23}	2^{16}
5512	256	2	2^{20}	2^{20}	2^{17}
	128	3.	2^{21}	2^{21}	2^{16}
	63	8	2^{25}	2^{25}	2^{17}

В табл. 8 наведено результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму. Довжина секретного та відкритого ключів визначається як $2 \times \mu_i \times l_h$, довжина ЕП $\mu_i \times l_h$.

В табл. 9 наведено значення ймовірностей нав'язування випадкових POTS одноразових ключів за умов та даних, що викладені в твердженнях 1 – 3.

Твердження 4. Нехай в POTS реалізується механізм та параметри ЕП, що викладені в твердженні 1, а щодо кожного w* блоку застосовується перетворення (26), причому щодо кожного байту $b_i^*(c_i)$ параметр w* приймає значення 2, 3. та 8 для геш-значення $h(l^*)$, де l^* довжина геш-значення, що отримане після виконання перетворення (26), тоді ймовірність нав'язування $P_н(w^*, l_h^*)$ хибного підписаного повідомлення на основі використання хибних випакових послідовностей, залежить від ймовірностей нав'язування w* блоку на усій довжині байт геш-значення l_h^* і визначається у

$$P_н(w^*, l_h^*) = 2^{-t^*} = 2^{-l_h^*/w^*} \tag{35}$$

Доведення та пояснення формули (25). При доведенні врахуємо, що геш-значення повідомлення M, що підписується, є випадковим, тому окремі блоки w* є незалежними і вони з'являються в ЕП випадково та рівноймовірно.

В табл. 9 наведено значення ймовірностей нав'язування w* блоків на усій довжині геш-значення l_h^*.

Таблиця 8

Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для POTS удосконаленого механізму

Розміри даних \lh, w_i			Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	μ_i	2	2^{10}	2^{10}	2^{9}
		3	2^{11}	2^{11}	2^{10}
		8	2^{12}	2^{12}	2^{11}
		16	2^{13}	2^{13}	2^{12}
		32	2^{14}	2^{14}	2^{13}
		128	2^{16}	2^{16}	2^{14}
		256	2^{17}	2^{17}	2^{16}
512	μ_i	2	2^{11}	2^{11}	2^{10}
		3	2^{12}	2^{12}	2^{11}
		8	2^{13}	2^{13}	2^{12}
		16	2^{14}	2^{14}	2^{13}
		32	2^{15}	2^{15}	2^{14}
		128	2^{17}	2^{17}	2^{16}
		256	2^{18}	2^{18}	2^{17}
		512	2^{19}	2^{19}	2^{18}

Таблиця 9

Ймовірності нав’язування випадкових POTS одноразових ключів $P_н(w^*, l_h^*)$

w* \ l_h*	1	2	3	8
512 біт (63. байт)	2^{-512}	2^{-256}	2^{-128}	2^{-64}
256 біт (32 байти)	2^{-256}	2^{-128}	2^{-64}	2^{-32}
128 біт (16 байт)	2^{-128}	2^{-64}	2^{-32}	2^{-16}

Висновки

1. Ідея механізму Вінтерніц полягає в тому, щоби підписувати, на відміну від *OTS* Лампорта, уже декілька бітів геш-значення, використовуючи одну послідовність *OTS* секретного одноразового ключа. Іншою особливістю механізму Вінтерніц є застосування однонаправлених функцій, які, на наш погляд, можна назвати функціями зчеплення. Особливістю застосування функцій зчеплення є можливість виділення відкритого ключа безпосередньо із отриманого ЕП. На наш погляд, це є принциповою особливістю механізму Вінтерніц.

2. Аналіз основних механізмів з одноразовими ключами – OTS Лампорта, OTS Вінтерніц ($WOTS$, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$) та модифікації механізму з одноразовими ключами (Biba, HORS, HORS+, HORS++ та HORST) не задовольняють вимогам просторової та часової складності, що суттєво ускладнює реалізацію постквантових ЕП на основі функцій гешування. В той же час, існує можливість побудування постквантових ЕП на основі OTS ключів, у вигляді perfekt OTS (POTS)[13].

3. Попередній аналіз показав, що вид функцій перетворення блоків (5) може суттєво вплинути та криптографічну стійкість проти існуючих та можливих атак. Тому, однією із важливих задач цього дослідження, є визначення функцій перетворення, які будуть дозволяти забезпечити зменшення довжин секретних та відкритих ключів, а також зменшувати довжину ЕП, забезпечуючи допустиму криптографічну стійкість проти існуючих та потенційних атак на основі класичних та квантових комп'ютерів.

4. При ЕП в механізмі PW-OTS застосовується перетворення кожного b_i блоку згідно з (25)), причому о b_i блок зашифровується (заміняється) послідовно секретним ключем із множини (12) X, інакше зашифровується (заміняється) послідовно секретним ключем із множини (12) Y. Правило (25) найбільш швидко може бути реалізоване засобом аналізу старшого біту, тобто 2^w. Якщо він має значення «1», то заміняється секретним ключем із множини (11) Y, інакше зашифровується (заміняється) послідовно секретним ключем із множини (12) X.

5. Порівняльний аналіз даних табл. 6 та 7 дозволяє зробити висновок, що при застосуванні механізму POTS розмір секретного та відкритого ключів може бути зменшений в 100 та більше разів. При цьому розмір ЕП також зменшується в 8 – 63 разів, що є суттєвим з урахуванням абсолютних значень довжин ЕП.

6. Необхідно відмітити, що для POTS механізму спостерігається зменшення криптографічної стійкості проти нав'язування хибних електронних підписів. Конкретні значення ймовірностей нав'язування $P_н(w^*, l_h^*)$ наведені в табл. 8. Їх аналіз дозволяє зробити висновок, що з урахуванням того, що PW-OTS є одноразовими, ймовірність 2^{-64} та і навіть 2^{-32} є достатніми.

7. Таким чином, наведені пропозиції з застосування POTS механізмів одноразових ключів та і, як наслідок, одноразових ЕП дозволяють зробити висновки про можливість їх застосування в постквантових механізмах ЕП на основі геш-функцій.

Список літератури: 1. *Koblitz Neal* A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes. – Режим доступу: https://eprint.iacr.org/2015/1018.pdf. 2. *Lily Chen* Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. – Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. 3. *Mosca M.* Setting the Scene for the ETSI Quantum-safe Cryptography Workshop" / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27. 4. *ETSI GR QSC 001* V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 5. *Горбенко І.Д., Кузнєцов О.О., Потій О.В., Горбенко Ю.І., Ганзя Р. С., Пономар В.А.* Постквантова криптографія та механізми її реалізації // Радиотехника. – 2016. – Вып. 186. – С. 32–52. 6. *Ralph Merkle*. A certified digital signature. In Gilles Brassard, editor, Advances inCryptology – CRYPTO '89, volume 3.35 of LNCS, pages 218–238. Springer, 1990. 7. *Leslie Lamport*. Constructing digital signatures from a one way function. Technical. Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979. 8. *Andreas Hülsing*. W-OTS+ – shorter signatures for hash-based signature schemes. In Amr Youssef, Abderrahmane Nitaj, and Aboul-Ella Hassanien, editors, Progress. in Cryptology – AFRICACRYPT 2013, volume 7918 of LNCS, pages 173–188.Springer, 2012. 9. *Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn*. SPHINCS: practical stateless hash-based Signatures. djb@cr.yp.to. daira@leastauthority.com, zooko@leastauthority.com. 10. *Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn*. SPHINCS: practical stateless hash-based Signatures. djb@cr.yp.to. daira@leastauthority.com, zooko@leastauthority.com. 11. *Gorbenko I., Ponomar V.* Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // Eastern European Journal of Enterprise Technologies, Volume 2, Issue 9-86, 2017, Pages 21-32.

http://journals.uran.ua/eejet/article/view/96321/93.881. 12. *ETSI* GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 13. *Аналіз* потенційних постквантових електронних підписів на основі геш-функцій / Ю.І.Горбенко, Т.В.Мельник, І.Д.Горбенко // Радиотехника. – 2017. – Вып. 189. – С. 115131. 14. *Анализ* постквантовых механизмов цифровой подписи на основе хеш-функций / Н.В.Ковалёва, И.Д. Горбенко // Прикладная радиоэлектроника. – 2016. – Т. 15. №3. – С. 000-000. 15. *Горбенко Ю.І.* ; за заг. ред. Горбенко І.Д. Методи побудування та аналізу, стандартизація та застосування КРСМ : монографія. – Харків : Форт, 2015. – 958с. 16. *Горбенко Ю.І., Ганзя Р.С.* Аналіз стійкості популярних криптоситем протиквантового криптоаналізу на основі алгоритму Гровера // Захист інформації. – 2014. – С. 22-28.

Акціонерне товариство
«Інститут інформаційних технологій»
Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 12.10.2017

УДК 681.3.06

Н.Е. ИВАНОВ, Р.В. ОЛЕЙНИКОВ, д-р техн. наук

ОЦЕНКА ПРОПУСКНОЙ СПОСОБНОСТИ ПЛАТФОРМЫ ETHEREUM НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СМАРТ-КОНТРАКТА

Введение

Децентрализованная платежная система (криптовалюта) Bitcoin стала первой платформой для учета виртуального актива, в которой клиенты и участники сети, не доверяя друг другу, способны приходить к единому консенсусу (согласованному состоянию балансов пользователей системы, истории транзакций и пр.). Для решения вопроса впервые была предложена технология блокчейн в качестве базы данных для узлов сети [1]. Успешное функционирование и возрастающая популярность платежной системы Bitcoin (капитализация Bitcoin составляет более 316 млрд долларов на 18.12.2017 [2]) увеличили интерес к используемым в ней решениям [1].

Новая технология блокчейн привнесла в распределенные системы доверие к данным, циркулирующим между узлами таких систем, и вызвала заметный интерес в финансовом секторе и других областях, непосредственно связанных с учетной деятельностью. Появление первой платформы, позволяющей разрабатывать полноценные программируемые смарт-контракты, Ethereum, открывает широкий потенциал в реальном создании и использовании децентрализованных приложений [3, 4].

Смарт-контракт – компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн. На платформе Ethereum смарт-контракт представляется в виде программного кода, корректное выполнение которого обеспечивается согласованием результатов его работы между узлами платформы [4].

Самым популярным смарт-контрактом в сети Ethereum является контракт начального размещения токенов (Initial Coin Offering, далее – ICO). Он служит для сбора средств в поддержку проектов финансирования стартапов и для эмиссии виртуальных активов – токенов [5]. Для понимания преимуществ, которые несет этот контракт, стоит обратить внимание на его типичные, но не обязательные, свойства и логику работы.

1) Пользователь отправляет на адрес контракта определенную сумму в виде криптовалюты Ethereum. В качестве вознаграждения ему отправляются виртуальные активы – токены. Таким образом обеспечивается распродажа токенов.

2) При сборе определенной суммы распродажа токенов прекращается.

3) При достижении определенной даты распродажа токенов прекращается.

4) Когда распродажа прекращается, если учредители не получили минимально необходимую сумму, то распродажа считается неудавшейся, и все пользователи, вложившие деньги, могут вернуть средства.

Компании, проводящие ICO для обеспечения интереса пользователей к инвестициям, могут наделить токены такими свойствами.

1) За токены можно приобрести продукт или услугу компании [5].

2) Владельцы токенов могут принимать участие в голосованиях внутри компании (digixDAO) [6].

3) Токены могут быть выведены на биржу (если соответствуют стандарту ERC20) и быть объектом торговли [7].

4) Владельцам токенов могут выплачивать дивиденды [8].

Для того чтобы быть более уверенными в успешном проведении ICO, компании прибегают к рекламным кампаниям. Иногда это приводит к чрезмерному количеству желающих участвовать в распродаже токенов. Количество транзакций, генерируемых ими, приводит к тому, что сети Ethereum приходится отклонять часть поступающих заявок [9]. В таком случае часть участников сети должны отправить свою транзакцию повторно и вновь ожидать подтверждения.

Анализ литературных данных и постановка проблемы

Главным недостатком блокчейн технологий является сложность их масштабирования и, соответственно, сравнительно низкая пропускная способность. Блокчейн технологии имеют ограничения по скорости обработки одной транзакции, а обрабатывающие узлы ограничены размером буфера транзакций. Оценка пропускной способности и вероятности отказа в обслуживании транзакций в платформе Ethereum позволит понять целесообразность использования смарт-контрактов. Теория систем массового обслуживания (СМО) предоставляет возможность произвести такие оценки и предоставить в итоге информацию о среднем времени ожидания операции в системе, вероятности отказа в обслуживании и зависимости этих величин от параметров системы: размера буфера ожидания, среднего времени обработки одной заявки [10].

Цель и задачи исследования

Целью работы является разработка математической модели для оценки пропускной способности платформы Ethereum, что позволит оценить, с каким уровнем нагрузки способна справиться платформа. Для достижения данной цели необходимо:

1) провести анализ условий, при которых функционирует глобальная платформа Ethereum;
2) определить параметры математической модели;
3) разработать математическую модель на основе СМО.

Анализ функционирования платформы ETHEREUM

На платформе Ethereum циркулируют множество транзакций, связанных с смарт-контрактами или же обычными криптовалютными переводами между пользователями. При разработке математической модели наличие этих транзакций не учитывается, поскольку они создают неравномерную и, в то же время, сравнительно незначительную нагрузку на сеть. Наибольшую же нагрузку сеть Ethereum испытывает во время проведения ICO распродаж. Транзакций, вызывающих код ICO контракта, в эти периоды подавляющее большинство, поскольку платформа Ethereum в первую очередь обрабатывает транзакции с более высокой комиссией, а остальные ставит в очередь или отбрасывает [4]. Для получения токенов раньше других участников распродажи, пользователи значительно увеличивают комиссию за транзакции, что приводит к тому, что некоторый промежуток времени большая часть подтверждаемых транзакций связана с эмиссией токенов [5]. Поэтому данное упрощение математической модели наиболее соответствует реальным процессам.

Разработка математической модели

Для согласования терминологий теории СМО и блокчейн, под транзакциями и заявками на обслуживания будем иметь в виду одно и то же.

Разработка математической модели СМО на основе платформы Ethereum включает в себя несколько допущений и упрощений.

1) Считается, что все транзакции, циркулирующие в системе, направлены на эмиссию новых токенов, ICO.

2) Принимается, что существует только один канал обслуживания. Несмотря на то, что сеть Ethereum – распределенная система, в итоговую базу данных блокчейн будет записан только один блок, от одного узла [4].

3) В математической модели не учитывается возникновение ветвлений (forks), так как различия будут в древовидной структуре блоков, а не в последовательностях транзакций.

4) Время генерации нового блока подчиняется экспоненциальному закону (коэффициент ковариации для этого закона – константа, равная единице) [4].

5) В блокчейн-платформе Ethereum нет максимально возможного размера блока и ограничения по количеству и размеру транзакции, однако существует ограничение на максималь-

ное количество газа (gas, комиссии за транзакцию), используемого в блоке. Эта величина может быть уменьшена или увеличена в следующем блоке на 20 процентов [4]. Это также позволяет в теории неограниченно увеличивать размер блока. При разработке математической модели принято, что максимальное количество транзакций в блоке будет равно 77. Это число взято из среднего количества транзакций в блоке реальной сети Ethereum [11], полученного по состоянию на ноябрь 2017 г.

6) Появление новых транзакций (другими словами, заявок) подчиняется простейшему закону распределения, а именно пуассоновскому.

В разрабатываемой математической модели считается, что поток входных заявок является простейшим, поскольку он соответствует свойствам стационарности, ординарности и отсутствию последействия в рассматриваемых условиях. Хотя ICO имеет различное количество заявок на протяжении всей распродажи на относительно небольших промежутках времени (1 – 10 минут), возникновение новой заявки будет стационарным. Каждая транзакция обрабатывается последовательно и имеет строгий порядок записи в децентрализованный блокчейн; благодаря этому обеспечивается ординарность потока заявок. При отказе сети Ethereum в обработке заявки пользователь повторно отправит транзакцию, однако в рассматриваемых нами коротких промежутках времени такого не произойдет, поскольку факт сбоя будет обнаружен пользователем не сразу, что позволяет представить повторный запрос как новую заявку, что обеспечивает свойство отсутствия последействия.

Рассмотрим формулу для подсчета среднего времени ожидания заявки [10]:

$$\omega = \frac{\lambda \times b^2 \times \left(1 + v^2\right)}{2 \times \left(1 - \lambda \times b\right)} \tag{1}$$

где λ – интенсивность потока заявок, b – среднее время обработки одной заявки, v – коэффициент вариации закона распределения среднего времени обработки одной заявки [10].

Знаменатель выражения показывает, что при $\lambda \times b$ больше или равным единице, среднее время ожидания выполнения одной заявки стремится к бесконечности. Действительно, если интенсивность слишком высока, то на бесконечном интервале заявка никогда не будет обработана [10].

Подсчитаны значения, соответствующие нашей блокчейн системе. Среднее время обработки одной заявки

$$b = \frac{\textit{среднее время нахождения блока}}{\textit{количество транзакций в блоке}} = \frac{15}{77} \approx 0{,}195\,\textit{сек}. \tag{2}$$

Среднее время нахождения блока и среднее количество транзакций блоке получено из среднестатистических характеристик реально работающей сети Ethereum на ноябрь 2017 года [11]. Коэффициент вариации для экспоненциального закона, определяющего время обработки одной заявки, равен единице. Таким образом, получим формулу среднего времени ожидания обработки одной заявки, зависящиго от интенсивности входного потока:

$$\omega = \frac{\lambda \times 0.038}{1 - \lambda \times 0.195} \tag{3}$$

Приведен график зависимости величины среднего времени ожидания одной заявки от интенсивности входных заявок (см.рис. 1).

Из графика следует, что при приближении интенсивности входного потока заявок к значению обратной величины среднего времени обработки b, среднее время ожидания заявки стремится к бесконечности. Однако для системы с наличием ограниченной очереди заявок такое значение интенсивности приведет к резкому увеличению вероятности в отказе обслуживания заявки.

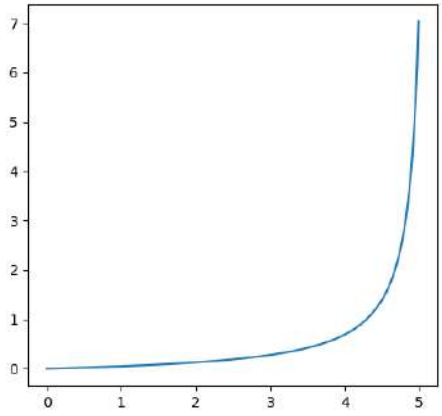


Рис. 1. График зависимости среднего времени ожидания обработки одной заявки к интенсивности входного потока заявок

Приведена формула вероятности того, что система с количеством каналов n, длиной очереди m будет заполнена на s заявок. Эта вероятность равна вероятности отказа заявке в обслуживании при наличии ограниченной очереди, когда s равно m [10]:

$$p_{n+s} = \frac{\frac{(\lambda \times b)^n}{n!} \times \left(\frac{\lambda \times b}{n}\right)^s}{\sum_{k=0}^{n} \frac{(\lambda \times b)^k}{k!} + \frac{(\lambda \times b)^n}{n!} \times \sum_{s=1}^{m} \left(\frac{\lambda \times b}{n}\right)^s} \quad (4)$$

Эта формула представляет собой обобщенный вид [10]. Для того чтобы получить вероятность отказа в обслуживании, необходимо подсчитать значения этой вероятности с предположением, что буфере размера m уже находится m заявок. Подставим значения для нашего случая: n=1, s=m, b=0.195:

$$p_{m+1} = \frac{(\lambda \times 0.195)^{m+1}}{1 + \lambda \times 0.195 + \sum_{s=1}^{m} (\lambda \times 0.195)^{s+1}} \quad (5)$$

Приведен график зависимости интенсивности поступающих заявок к вероятности отказа заявке в обслуживании при размере буфера, равном m=100 (рис. 2). Размер буфера выбран таким, поскольку, хотя размер буфера значительно больше у реальных узлов, его увеличение не повлияет на график существенным образом, однако осложнит вычисления, что будет показано в дальнейшем анализе.

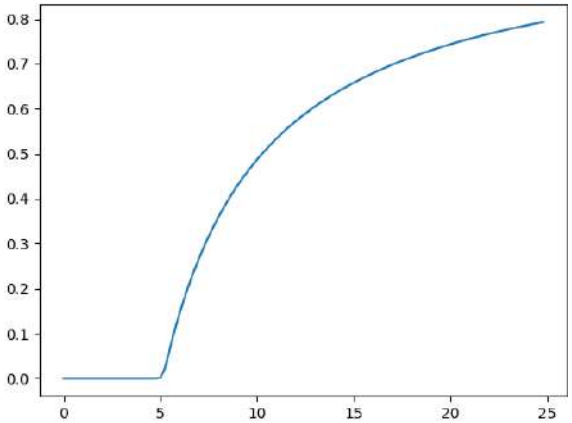


Рис. 2. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок

Обсуждение результатов исследования модели

Из приведенных формул и графиков можно выделить параметры, которые влияют на такие характеристики системы, как среднее время ожидания заявки на обработку и вероятность отказа в обслуживании заявки:

1) среднее время обработки одной заявки – *b*;
2) размер буфера заявок – *m*;
3) количество каналов обработки заявок – *n*;
4) интенсивность входного потока заявок – λ.

При этом интенсивность входного потока λ не является той величиной, которая может быть урегулирована разработчиками системы и является параметром среды, в котором функционирует система. Тогда улучшение характеристик системы может быть достигнуто тремя способами:

1) увеличением буфера заявок;
2) уменьшением среднего времени обработки одной заявки;
3) увеличением количества каналов параллельной обработки заявок.

Увеличение буфера заявок может быть достигнуто увеличением оперативной памяти вычислительных узлов сети. Уменьшение среднего времени обработки одной заявки и увеличение числа каналов требуют переработки самого протокола консенсуса блокчейн систем [3]. Проанализируем как изменение данных параметров влияет на вероятность отказа заявки в обслуживании.

Ниже приведена зависимость этой величины от размера буфера, равного 1, 3, 10, 100 и 1000 заявок с фиксированным значением среднего времени обработки одной заявки b=0.195 (рис. 3).

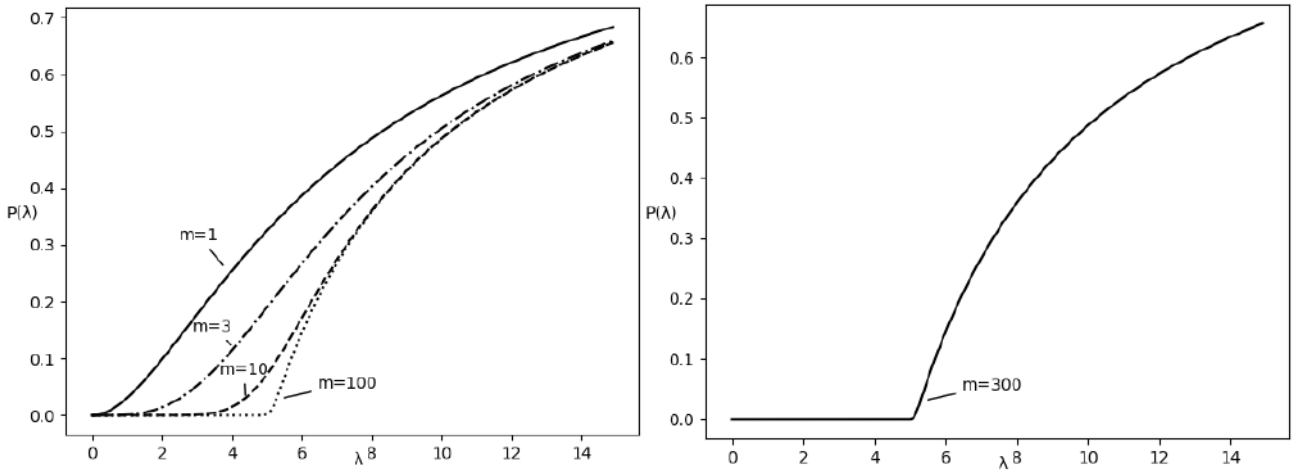


Рис. 3. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок при *m*=1,3,10,100,300

Из полученных графиков следует, что увеличение размера буфера ожидания заявок имеет свой предел по улучшению эффективности работы системы. На графиках с размером буфера *m*=1, 3, 10 заметен сдвиг и уменьшение сглаженности перехода к моменту резкого увеличения вероятности отказа заявки в обслуживании при больших значениях интенсивности входного потока заявок. Однако анализ графиков с размером буфера *m*=100, 300 свидетельствует, что они существенно не отличаются. Таким образом, размер буфера после определенного значения не повышает эффективность системы.

Стоит дополнительно отметить, что на практике больший размер буфера позволит системе преодолеть моменты неожиданного и резкого увеличения количества транзакций на некотором локальном промежутке времени. Время ожидания обработки транзакций будет

значительно больше, однако это позволит сохранить большее количество транзакций пользователей в системе без необходимости в их повторной отправке, что повышает надежность используемой системы.

Приведены графики вероятности отказа заявки в обслуживании с фиксированным размером буфера заявок m=100 и средним временем обработки одной заявки b=0.5, 0.1, 0.05 (см. рис. 4).

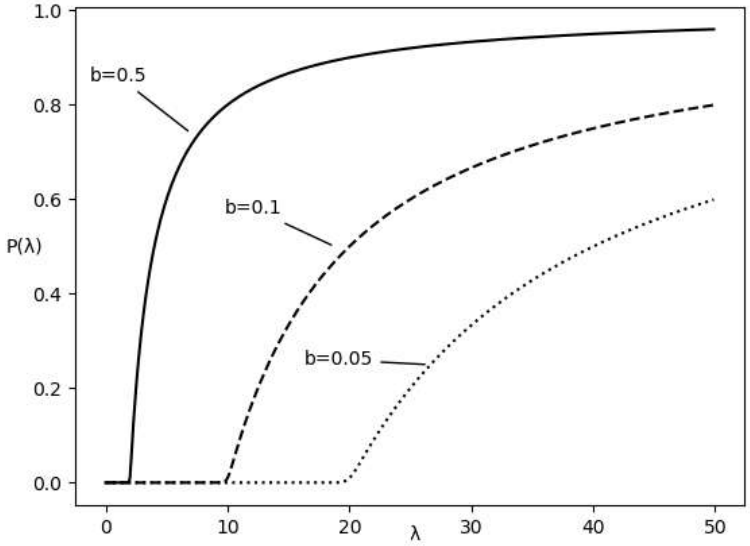


Рис. 4. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок при b = 0.5, 0.1, 0.05

На основе этих графиков можно сделать вывод, что уменьшение среднего времени обработки транзакции позволяет отодвинуть момент резкого повышения вероятности отказа системы в обслуживания до больших значений интенсивности входного потока заявок. Кроме того, зависимость этих величин обратно пропорциональна друг другу. Из этого следует, что от уменьшения среднего времени обработки транзакции в системе пропускная способность системы всегда будет увеличиваться. Однако добиться этого улучшения значительно сложнее, так как для улучшения этой характеристики необходимо усовершенствовать протокол нахождения консенсуса между узлами сети, что представляет из себя значительно более трудную задачу, требующую сложных теоретических исследований и тестирования прототипов.

Увеличение количества каналов обработки заявок улучшает параметры системы аналогично уменьшению среднего времени обслуживания одной заявки таким образом, что система с двумя каналами и средним временем обслуживания заявки b эквивалентна системе с одним каналом и средним временем обслуживания одной заявки $b/2$ (соответственно, графики для данного случая не приводятся). Команда разработчиков платформы Ethereum считает увеличение количества каналов блокчейн-технологий наиболее перспективным среди всех остальных и уже ведут разработки в этом направлении. Это улучшение называется Ethereum Plasma [12].

Выводы

Разработана математическая модель смарт-контракта ICO на основе платформы Ethereum, ориентированная на анализ проблемы низкой пропускной способности блокчейн-систем. Характеристики модели зависят от таких параметров как размер буфера транзакций, среднее время обработки одной транзакции и количество каналов обслуживания. Исходя из данных характеристик модель позволяет определить вероятность отказа транзакции в обслуживании в зависимости от интенсивности входящего потока заявок, на основании чего организаторы ICO могут прогнозировать максимально допустимую нагрузку на сеть.

Кроме того, на основе анализа зависимостей характеристик модели от параметров было установлено, что решение проблемы масштабируемости блокчейн-технологий возможно только благодаря уменьшению среднего времени обработки одной транзакции либо увеличению количества каналов, для чего необходима модернизации алгоритма консенсуса и применения технологий, подобных Lightning Network [13].

Список литературы: 1. *Why Bitcoin* Matters [Электронный ресурс]/ Marc Andreessen. – Режим доступа: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters – 15.11.2017 – Загл. с экрана. 2. *Cryptocurrency* Market Capitalizations [Электронный ресурс]/ Coinmarketcup team. – Режим доступа: https://coinmarketcap.com/ - 18.12.2017 – Загл. с экрана. 3. *Ether Sale*: A Statistical Overview [Электронный ресурс]/ Vitalik Buterin – Режим доступа: https://blog.ethereum.org/ether-sale-a-statistical-overview- 15.11.2017 – Загл. с экрана. 4. *Ethereum* white-paper [Электронный ресурс] /Ethereum Foundation – Режим доступа: https://bitcoil.co.il/Doublespend.pdf – 15.11.2017 – Загл. с экрана. 5. *Initial Coin* Offering (ICO) [Электронный ресурс]/ Investopedia team – Режим доступа: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp – 15.11.2017 – Загл. с экрана. 6. *Digix's* Whitepaper: The Gold Standard in Crypto-Assets [Электронный ресурс]/ Anthony C. Eufemio, Kai C. Chng, Shaun Djie – Режим доступа: https://digix.global/whitepaper.pdf – 15.11.2017 – Загл. с экрана. 7. *What is ERC-20* and What Does it Mean for Ethereum [Электронный ресурс]/ Nathan Reiff – Режим доступа: https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum – 15.11.2017 – Загл. с экрана. 8. *What are Polybius* tokens and why should they be in every crypto-investor's portfolio [Электронный ресурс]/ Polybius team – Режим доступа: https://blog.polybius.io/what-are-polybius-tokens-and-why-should-they-be-in-every-crypto-investors-portfolio-73a813c77429 – 15.11.2017 – Загл. с экрана. 9. *How the status* ico almost crashed the ethereum network [Электронный ресурс]/ Ashour Iesho – Режим доступа: http://bitcoinist.com/how-the-status-ico-almost-crashed-the-ethereum-network – 15.11.2017 – Загл. с экрана. 10. *Вентцель Е.С.* Теория Вероятностей. - М., 1969. 576 с. 11. *Ethereum* network statistic [Электронный ресурс] – Режим доступа: https://ethstats.net – 15.11.2017 – Загл. с экрана. 12. *Plasma:* Scalable Autonomous Smart Contracts [Электронный ресурс]/ Joseph Poon, Vitalik Buterin – Режим доступа: https://plasma.io/plasma.pdf – 15.11.2017 – Загл. с экрана. 13 *The Bitcoin* Lightning Network: Scalable Off-Chain Instant Payments [Электронный ресурс]/ Joseph Poon, Thaddeus Dryja – Режим доступа: https://lightning.network/lightning-network-paper.pdf – 15.11.2017 – Загл. с экрана.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 09.11.2017

УДК 621.3.06

М.Ю. РОДІНКО, Р.В. ОЛІЙНИКОВ, д-р техн. наук

МЕТОДИ ПОШУКУ ДИФЕРЕНЦІЙНИХ ХАРАКТЕРИСТИК ЦИКЛОВОЇ ФУНКЦІЇ СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУ «КИПАРИС»

Вступ

Малоресурсна криптографія [1] є одним з найпопулярніших напрямків у сучасній криптології, орієнтованим на розробку симетричних примітивів, що мають високу швидкодію перетворень та компактну реалізацію на різних платформах. З метою забезпечення цих вимог розробники відходять від традиційних методів побудови симетричних шифрів (зокрема заснованих на застосуванні таблиць підстановок – S-блоків) та все більше звертаються до простих операцій таких, як модульне додавання, циклічний зсув та XOR. Подібна архітектура отримала назву ARX (Addittion-Rotation-XOR) та знайшла застосування у таких відомих симетричних шифрах як SIMON [2], SPECK [3], Salsa20 [4], ChaCha20 [5] та ін.

Із урахуванням останніх тенденцій малоресурсної криптографії на основі ARX-перетворень був розроблений симетричний блоковий шифр «Кипарис» [6]. Розроблений шифр має високу швидкодію перетворень, компактну реалізацію, підтримує довжину ключа, достатню для забезпечення стійкості у постквантовий період (256 та 512 біт). Первинний аналіз алгоритму, що включав статистичне тестування та оцінку лавинних показників, показав, що блоковий шифр «Кипарис» задовольняє цим властивостям. Тепер нагальним питанням є обґрунтування стійкості шифру до найбільш відомої та ефективної атаки на блокові шифри – диференційного криптоаналізу [7].

Однак, якщо для шифрів, заснованих на S-блоках, існує загальний підхід до обґрунтування стійкості до диференційного (а також і лінійного) криптоаналізу, то для ARX-подібних примітивів такого підходу немає. Через велику кількість повторів простих операцій дуже складно представити математичне обґрунтування навіть окремого алгоритму. Зазвичай, ARX-подібна конструкція є скоріш інтуїтивною, ніж математично обґрунтованою.

Традиційно стійкість блокового шифру до диференційного криптоаналізу визначається верхньою границею ймовірності диференційної характеристики (ДХ). У статті пропонується три підходи до знаходження найбільш ймовірної диференційної характеристики блокового шифру «Кипарис».

1. Алгоритм блокового шифрування «Кипарис»

Алгоритм шифрування «Кипарис» [6] виконує перетворення блоків даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l,k \in \{256,512\}$, $l = k$. Операції виконуються над s-бітними словами, $s \in \{32,64\}$.

На вхід процедури зашифрування подається блок відкритого тексту $P = (P_0, P_1, ..., P_7)$ та циклові ключі $RK^{(0)}, RK^{(1)}, \ldots, RK^{(t-1)}$. Блок відкритого тексту P ділиться на два підблока: $L_0 = (P_0, P_1, P_2, P_3)$, $R_0 = (P_4, P_5, P_6, P_7)$. Вихід i-ї ітерації перетворення обчислюється як:

$$L_i = R_{i-1} \oplus F\left(L_{i-1}, RK^{(i-1)}\right),$$

$$R_i = L_{i-1}.$$

Циклова функція F представляє собою додавання підблока L_{i-1} з ключем $RK^{(i-1)}$ за модулем 2 та двократне повторення функції $h(P_0', P_1', P_2', P_3')$, на вхід якої подається чотири s-бітних слова. Вихідне значення функції h обчислюється як:

$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r1),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r2),$$
$$P_0' = ADD(P_0', P_1'),\ P_3' = XOR(P_3', P_0'),\ P_3' = ROTL(P_3', r3),$$
$$P_2' = ADD(P_2', P_3'),\ P_1' = XOR(P_1', P_2'),\ P_1' = ROTL(P_1', r4),$$

де $ADD(x, y)$ – додавання за модулем s двох s-бітних слів; $XOR(x, y)$ – XOR двох s-бітних слів; $ROTL(x, r)$ – циклічний зсув s-бітного слова вліво на r біт.

2. Диференційні властивості операції модульного додавання

Як відомо, для знаходження диференційних характеристик шифру використовують таблицю розподілу різниць (ТРР) нелінійного перетворення. Таким перетворенням у ARX-подібному шифрі є операція додавання за модулем 2^n.

Диференційна ймовірність додавання за модулем 2^n (xdp^+) – це ймовірність, з якою вхідні різниці α та β переходять у вихідну різницю γ через застосування операції модульного додавання, обчислена для всіх можливих пар n-бітних входів [8]:

$$xdp^+(\alpha, \beta \to \gamma) = 2^{-2n} \times \#\{(x, y) : ((x \oplus \alpha) + (y \oplus \beta)) \oplus (x + y) = \gamma\}.$$

У [9] запропонований швидкий алгоритм для обчислення xdp^+, заснований на S-функціях.

У разі, якщо в якості нелінійної функції шифру виступає S-блок, побудувати ТРР дуже легко, оскільки для S-блока байт-в-байт така таблиця містить всього 256×256 елементів. Для додавання за модулем 2^{32} або більше побудувати повну ТРР не представляється можливим (розмір ТРР для додавання за модулем 2^{32} складає 2^{64}). Підхід до вирішення цієї проблеми представлений у [8], де пропонується будувати так звану часткову таблицю розподілу різниць (англ. partial difference distribution table, pDDT), що містить диференціали $(\alpha, \beta \to \gamma)$ з імовірністю p_{thres} рівною або вищою заданої:

$$(\alpha, \beta, \gamma) \in D \Leftrightarrow DP(\alpha, \beta \to \gamma) \geq p_{thres}.$$

У [8] наведено приклади побудування часткових таблиць для 32-бітових циклових функцій SPECK, XTEA.

Об'єднуючи часткові таблиці для різних компонентів циклової функції, автори будують часткову таблицю для всієї циклової функції, які використовують в модифікованому алгоритмі Мацуї для побудови багатоциклових ДХ [8].

3. Методи пошуку диференційних характеристик циклової функції блокового шифру «Кипарис»

3.1. Прямий метод пошуку ДХ

Особливістю шифру «Кипарис» є те, що циклова функція оперує $l/2$-бітними блоками даних, де $l \in \{256, 512\}$, тому побудування часткової таблиці для всієї циклової функції є складною задачею. У даному випадку, найбільш очевидним видається метод пошуку характеристик, що полягає в наступному.

1) Обрати множину $l/2$-бітних вхідних різниць Ξ.

2) Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ (ξ_i, ψ_i), де ψ_i – різниця на виході циклової функції. При цьому на j-му з восьми суматорів обирати найбільш ймовірний перехід $\max(\alpha_j, \beta_j \to \gamma_j)$.

3) Імовірність знайденої ДХ $p(\xi_i \to \psi_i)$ обчислити як добуток ймовірностей перетворення на восьми суматорах:

$$p(\xi_i \to \psi_i) = \prod_{j=1}^{8} p(\alpha_j, \beta_j \to \gamma_j) \quad (1)$$

Головним питанням є вибір множини Ξ. Аналіз часткової таблиці для додавання за модулем 2^{32} показав, що ймовірність перетворення на суматорі зростає зі зменшенням кількості активних біт на вході. Так, наприклад для суматора за модулем 2^{32} та $p(\alpha, \beta \to \gamma) \geq 1/2$, максимальна кількість активних біт у вхідній різниці (α, β) складає 2 біти. У зв'язку із цим, з метою мінімізації кількості активних біт на входах суматорів циклової функції, до множини Ξ доцільно включати вхідні різниці:

- з мінімальною вагою Хемінга, наприклад такі, що мають по одному активному біту в одному, двох або трьох s-бітних словах;
- базуючись на найбільш ймовірних переходах часткової ТРР для суматора.

У результаті, за допомогою запропонованого методу для 256-бітової циклової функції шифру «Кипарис» була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-12}$ (табл. 1).

Таблиця 1

Параметри ДХ циклової функції шифру «Кипарис»

Вхідна різниця (hex)	80000000 80000000 80000000 0
Вихідна різниця (hex)	40844 26260262 C4484400 44084400
Ймовірність ($\log_2 p$)	-12

3.2. Метод пошуку ДХ «у двох напрямках»

Вибір вхідних різниць з мінімальною кількістю активних бітів хоч і дозволяє дещо збільшити загальну ймовірність характеристики, проте, завдяки дифузії, навіть один активний біт на вході циклової функції вже на середині перетворення активує достатньо велику кількість бітів. Як було вказано вище, циклова функція F представляє собою дві ітерації функції h. З метою активізації якомога меншого числа бітів на входах суматорів пропонується оптимізація представленого вище методу, що полягає в наступному.

1) Обрати множину $l/2$-бітних різниць Ξ тим самим способом, що й у попередньому методі.

2) Кожну різницю $\xi_i \in \Xi$ розглядати як вихід першої та вхід другої ітерації функції h. Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ для функції h та її інверсії h^{-1}. ДХ для циклової функції F буде представляти об'єднання характеристик для h^{-1} та h.

3) Імовірність ДХ $p(\xi_i \to \psi_i)$ для циклової функції F обчислити як добуток на восьми суматорах за формулою (1).

Цей метод дозволив значно покращити попередній результат: для 256-бітової циклової функції шифру була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-3}$ (табл. 2).

Таблиця 2

Параметри ДХ циклової функції, отриманої за допомогою методу пошуку «у двох напрямках»

Вхідна різниця (hex)	80000 80080000 80000000 80000000
Вихідна різниця (hex)	800 4040040 80080000 80000
Ймовірність ($\log_2 p$)	-3

Представлений метод все одно не гарантує, що знайдена ДХ є найкращою, і не існує інших ДХ з більшою ймовірністю.

3.3. Оптимізований метод пошуку найкращої ДХ циклової функції

Відмітимо, що для знайденої вище ДХ, ймовірність перетворення на суматорі $p(\alpha_j, \beta_j \to \gamma_j) \geq 1/2$. Цей факт дозволяє стверджувати, що якщо існує якась ДХ, краща за

знайдену, то вона також буде містити переходи на суматорах з імовірністю, не менше ½. Таким чином, множину вхідних різниць Ξ можна суттєво обмежити, вибравши вхідні різниці таким чином, щоб ймовірність перетворення на перших двох суматорах була не менше ½. Це дозволить знайти ДХ з високою ймовірністю, яка існує для циклової функції. Новий метод складається з наступних кроків.

1) Побудувати ТРР для операції додавання за модулем 2^n, що містить переходи з імовірністю $p(\alpha_j, \beta_j \to \gamma_j) \geq 1/2$.

2) Враховуючи, що кожна вхідна різниця $\xi_i \in \Xi$ складається з чотирьох s-бітних слів $\xi_i = \left\{\xi_i^{(0)}, \xi_i^{(1)}, \xi_i^{(2)}, \xi_i^{(3)}\right\}$, множину вхідних різниць Ξ сформувати за допомогою алгоритму, наведеного на рис. 1.

$$
\begin{aligned}
&\textit{for each } (\alpha_j, \beta_j \to \gamma_j) \textit{ from pDDT}\\
&\xi_i^{(0)} = \alpha_j; \xi_i^{(1)} = \beta_j;\\
&\textit{for each } (\alpha_k, \beta_k \to \gamma_k) \textit{ from pDDT}\\
&\xi_i^{(2)} = \alpha_k; \xi_i^{(3)} = XOR(\gamma_j, ROTR(\beta_k, 16));
\end{aligned}
$$

Рис. 1. Алгоритм вибору вхідних різниць

3) Для кожної вхідної різниці $\xi_i \in \Xi$ побудувати ДХ (ξ_i, ψ_i). Імовірність ДХ $p(\xi_i \to \psi_i)$ для циклової функції F обчислюється як добуток на восьми суматорах за формулою (1).

Цей метод дозволив ще покращити попередній результат: для 256-бітової циклової функції шифру була знайдена ДХ з імовірністю $p(\xi \to \psi) = 2^{-2}$ (табл. 3).

Таблиця 3

Параметри ДХ циклової функції, отриманої за допомогою оптимізованого методу

Вхідна різниця (hex)	0 80000000 800000 80008080
Вихідна різниця (hex)	80000000 4000 80 80
Ймовірність ($\log_2 p$)	-2

У табл. 4 представлені переходи на суматорах, що складають отриману характеристику.

Таблиця 4

Ймовірності переходів на восьми суматорах

Номер суматора	$(\alpha, \beta) \to \gamma$		p
1	(0, 80000000)	→ 80000000	1
2	(800000, 80800000)	→ 80000000	1/2
3	(80000000, 0)	→ 80000000	1
4	(80000000, 80000000)	→ 0	1
5	(80000000, 0)	→ 80000000	1
6	(0, 0)	→ 0	1
7	(80000000, 0)	→ 80000000	1
8	(80, 0)	→ 80	1/2

З табл. 4 можна помітити, що старший активний біт різниці не впливає на ймовірність переходу, а у випадку $p = 1/2$ вхідна різниця містить один активний біт, не враховуючи старший.

Висновки

Таким чином, запропоновано три методи пошуку диференційних характеристик циклової функції блокового шифру «Кипарис»: прямий метод пошуку, метод пошуку «у двох напрямках» та оптимізований метод пошуку диференційної характеристики з високою ймовірністю. Метою всіх трьох підходів є активізація найменшої кількості біт на входах суматорів циклової функції, що, в свою чергу, збільшує ймовірність заданого перетворення. Останній із запропонованих методів дозволив знайти диференційну характеристику на циклову функцію блокового шифру «Кипарис» з ймовірністю, що дорівнює ¼.

Список літератури: 1. *Mouha, Nicky*. The Design Space of Lightweight Cryptography [Text] / Nicky Mouha // NIST Lightweight Cryptography Workshop 2015. – 2015. – 19 p. 2. *Beaulieu R. et al*. The SIMON and SPECK lightweight block ciphers // Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE // IEEE, 2015. – С. 1-6. 3. *Bernstein D. J*. The Salsa20 family of stream ciphers Salsa. – 2007. 4. *Bernstein D. J*. ChaCha, a Variant of Salsa // Workshop Record of SASC: The State of the Art of Stream Ciphers. 6. *Родінко М.Ю., Олійников Р.В*. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» // Радіотехніка. – 2017. – Вип. 189. – С. 100-107. 7. *Biham, E*. Differential Cryptanalysis of DES-like Cryptosystem / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – Vol. 4. – P. 3-72. 8. *Biryukov A., Velichkov V*. Automatic Search for Differential Trails in ARX Ciphers //CT-RSA. – 2014. – Т. 8366. – С. 227-250. 9. *Mouha N. et al*. The Differential Analysis of S-Functions // Selected Areas in Cryptography. – 2010. – V. 6544. – P. 36-56.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 12.11.2017

УДК 004.056.55

О.О. КУЗНЕЦОВ, д-р техн. наук, Д.В. ІВАНЕНКО, канд. техн. наук, М.С. ЛУЦЕНКО, В.А. ТИМЧЕНКО, О.М. МЕЛКОЗЕРОВА, канд. техн. наук, М.О. ОСАДЧУК, Є.В. ОСТРЯНСЬКА

ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ АЛГОРИТМІВ ПОТОКОВОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

Вступ

Потокові алгоритми криптографічного перетворення знайшли широке застосування та впровадження для захисту важливих інформаційних ресурсів, зокрема, таємної інформації, що є власністю держави, персональних даних, комерційної таємниці та інших відомостей, захист яких передбачено діючим законодавством [1, 2]. Основними перевагами потокового криптоперетворення є підвищена безпека та швидкодія [1 – 4], і це робить їх застосування найбільш доцільним для захисту каналів управління та зв'язку у військовій сфері, державному управлінні, банківському секторі та ін. Отже розробка, дослідження, впровадження та експлуатація засобів потокового шифрування є надзвичайно важливою та актуальною проблемою загальнодержавного значення з розбудови національної інформаційної інфраструктури та створення передових інформаційних технологій. Стандартизований на національному та/або міжнародному рівнях криптоалгоритм повинен забезпечувати високій рівень стійкості (в тому числі і в умовах можливого застосування квантового криптоаналізу), мати високу швидкодію та ефективно функціонувати на різних обчислювальних платформах [5 – 9].

В цій роботі викладаються основні результати порівняльних досліджень алгоритмів потокового криптографічного перетворення, зокрема стандартизованих на міжнародному рівні у ISO/IEC 18033-4 [6] та ISO/IEC 29192-3 [7], представлених у якості переможців міжнародного проекту eSTREAM з виявлення нових поточних шифрів придатних для широкого застосування у Європейському Союзі [8], та з проекту CRYPTREC (Cryptography Research and Evaluation Committees), заснованому японським урядом для оцінки і рекомендації шифрувальних методів для урядового і індустріального використання [9]. Перелік досліджуваних алгоритмів потокового криптоперетворення наведено у табл. 1, де вказано короткі відомості про шифри та належність до відповідних стандартів чи проектів. До порівняння долучено також алгоритми потокового симетричного шифрування (ПСШ) «Струмок» (STRUMOK) [10, 11] та RC4 [12 – 14], а також всесвітньовідомий блоковий симетричний шифр AES, що стандартизований на національному рівні в США (FIPS-197) [15] та на міжнародному рівні у ISO/IEC 18033-3 [16]. У певних режимах блоковий алгоритм AES може функціонувати як генератор ключових потоків.

Таблиця 1

Перелік досліджуваних алгоритмів потокового криптографічного перетворення

Назва шифру	Специфіковано	Розмір стану, біт	Розмір ключа, біт	Розмір IV, біт
AES-128	FIPS-197 [15], ISO/IEC 18033-3 [16], CRYPTREC [9]	128	128	128
AES-256		256	256	256
HC-128	eSTREAM [8]	128	128	128
HC-256		256	256	256
MICKEY-128	eSTREAM [8]	160	128	128
RABBIT	ISO/IEC 18033-4 [6], eSTREAM [8]	513	128	64
SALSA-20	eSTREAM [8]	512	128	64
SNOW2.0-128	ISO/IEC 18033-4 [6]	512	128	128
SNOW2.0-256	ISO/IEC 18033-4 [6]	512	256	256

SOSEMANUK	eSTREAM [8]	512	128	128
STRUMOK 256	[10, 11]	1024	256	256
STRUMOK 512	[10, 11]	1024	512	512
TRIVIUM	eSTREAM [8]	288	80	80
CRYPTMT3	eSTREAM [8]	128	128	64
DECIM-128	ISO/IEC 18033-4 [6], eSTREAM [8]	288	128	128
RC4	[12 – 14]	256	256	–
KCIPHER-2	ISO/IEC 18033-4 [6], CRYPTREC [9]	640	128	128
GRAIN	eSTREAM [8]	128	128	96
MUGI	ISO/IEC 18033-4 [6]	128	128	128

Порівняльні дослідження алгоритмів з табл. 1 проводилися за двома напрямками. По-перше, досліджувалася статистична безпека шляхом тестування вихідних послідовностей (генерованих ключових потоків). Для цього застосовано методики статистичного тестування NIST Statistical Test Suite (NIST STS) [17 – 19] та DIEHARD [20, 21]. По-друге, досліджувалася швидкодія відповідних генераторів у певних режимах (за методикою тестування, яку було запропоновано при проведенні конкурсу eSTREAM [8]). Отримані результати досліджуються з метою визначення перспективного напрямку подальших розробок та обґрунтування нового потокового шифру в Україні.

Порівняльні дослідження статистичної безпеки алгоритмів потокового шифрування

Для проведення експериментальних досліджень криптографічних властивостей потокового симетричного криптоперетворення в цій роботі використано статистичне тестування вихідних послідовностей (ключового потоку або гами шифрувальної). До найбільш відомих наборів статистичних тестів належать [17 – 21]:

– DIEHARD. Найбільш ранній і відомий набір тестів. Він містить 12 статистичних тестів;

– NIST Statistical Test Suite (NIST STS) розроблений Національним інститутом стандартів і технологій США. До його складу входять 15 статистичних тестів.

Пакет статистичного тестування NIST STS був розроблений в ході проведення конкурсу AES для дослідження генераторів випадкових або псевдовипадкових послідовностей (ПВП) і є найбільш поширеним інструментом оцінки статистичної безпеки криптографічних примітивів.

Порядок тестування окремої двійкової послідовності S має наступний вид [18]:

– висувається нульова гіпотеза H_0 – припущення про те, що дана двійкова послідовність S є випадковою;

– за послідовністю S розраховується статистика тесту $c(S)$;

– з використанням спеціальної функції та статистики тесту розраховується значення ймовірності $P = f(c(S))$;

– значення ймовірності P порівнюється з пороговим значенням $\alpha \in [0{,}96; 0{,}99]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

Пакет містить 15 статистичних тестів:

1) *Частотний побітовий тест*. Тест оцінює, на скільки близькою є доля одиниць до 0,5.

2) *Частотний блоковий тест*. Суть тесту полягає у визначенні долі одиниць всередині блоку довжиною m бітів.

3) *Тест на послідовність однакових бітів*. В даному тесті необхідно з'ясувати, чи дійсно кількість неперервних послідовностей однакових бітів відповідає їх кількості у випадковій послідовності.

4) *Тест на найдовшу послідовність одиниць в блоці*. В даному тесті визначається найдовший рядок одиниць всередині блоку довжиною m бітів, перевіряється відповідність очікуваній довжини найдовшого рядку одиниць у випадковій послідовності.

5) *Тест рангів бінарних матриць*. Метою цього тесту є перевірка на лінійну залежність підрядків фіксованої довжини, що складають початкову послідовність. Даний тест також є в пакеті DIEHARD [20, 21].

6) *Спектральний тест*. Суть тесту полягає в оцінці висоти піків дискретного перетворення Фур'є початкової послідовності. Метою є виявлення періодичних властивостей вхідної послідовності.

7) *Тест на співпадіння шаблонів, що не перекриваються*. В даному тесті підраховується кількість заздалегідь визначених шаблонів, які знайдені в початковій послідовності. Необхідно виявити генератори випадкових або псевдовипадкових чисел, що формують занадто часто задані неперіодичні шаблони.

8) *Тест на співпадіння шаблонів, що перекриваються*. Суть даного тесту полягає в підрахунку кількості заздалегідь визначених шаблонів, які знайдені в початковій послідовності.

9) *Універсальний статистичний тест Маурера*. Тут визначається число бітів між однаковими шаблонами в початковій послідовності (міра, що має безпосереднє відношення до довжини стиснутої послідовності).

10) *Тест на лінійну складність*. В основі тесту лежить принцип роботи лінійного регістра зсуву зі зворотним зв'язком. Необхідно з'ясувати, чи є вхідна послідовність досить складною для того, щоб вважатися випадковою.

11) *Тест на періодичність*. Даний тест полягає в підрахунку частоти всіх можливих перекривань шаблонів довжини m бітів протягом початкової послідовності бітів.

12) *Тест приблизної ентропії*. Акцент робиться на підрахунку частоти всіх можливих перекривань шаблонів довжини m бітів протягом початкової послідовності бітів.

13) *Тест кумулятивних сум*. Необхідно визначити, чи є кумулятивна сума часткових послідовностей, що виникають у вхідний послідовності, занадто великою або занадто маленькою у порівнянні з очікуваною поведінкою такої суми для випадкової вхідної послідовності.

14) *Тест на довільні відхилення*. Суть даного тесту полягає в підрахунку числа циклів, що мають суворо k відвідувань при довільному обході кумулятивної суми. Мета тесту полягає у визначенні того, чи відрізняється число відвідувань певного стану всередині циклу від аналогічного числа в разі випадкової вхідної послідовності.

15) *Інший тест на довільні відхилення*. У цьому тесті підраховується загальна кількість відвідувань певного стану при довільному обході кумулятивної суми.

Проходження кожного з 15 статистичних тестів є важливим критерієм оцінки псевдовипадкового генератору. Тому навіть не відповідність за одним чи більше критеріями означає, що ключовий потік не може на високому рівні протистояти криптоаналізу. Якщо, з іншого боку, генератор проходить всі тести, це зовсім не говорить про захищеність генератору, оскільки такі тести не враховують особливостей реальної конструкції генератору.

За методикою NIST STS для 15 наведених вище тестів в залежності від вхідних параметрів обчислюються 188 значень ймовірності P. Таким чином, в результаті тестування двійкової послідовності формується вектор $P=\{P_1,P_2...P_{188}\}$ значень ймовірностей. Аналіз складових P_j цього вектору дозволяють вказати на конкретні дефекти випадковості протестованої послідовності.

Відповідно до методики статистичного тестування [19] були проведені експериментальні дослідження криптографічних властивостей різних ПСШ. В роботі були протестовані ключові потоки сучасних потокових шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Trivium та запропонованого в [10, 11] шифру «Струмок». Для статистичного тестування парою випадковий ключ K/випадковий вектор ініціалізації IV було згенеровано 100 послідовностей завдовжки 10^6 біт. Оцінювалося математичне сподівання числа пройдених тестів досліджуваним генератором. Результати випробувань наведені в табл. 2.

Таблиця 2

Результати статистичного тестування для шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Strumok, Trivium

Назва алгоритму	M099	D099	S099	P099	M096	D096	S096	P096	MIN
AES-128	127,07	20,456	4,438	1.00	186,63	0,3191	0,554	1.00	185
CRYPTMT	130,89	52,988	7,279	1.00	158,56	5,284	2,299	1.00	181
DECIM	132,44	19,358	4,399	1.00	186,44	0,9136	0,956	1.00	185
ENOCORO	132,92	51,22	7,157	1.00	187,17	0,79	0,89	1.00	185
GRAIN	132,36	57,32	7,571	1,00	186,92	1,414	1,185	1.00	182
HC-256	133,75	36,44	6,04	1,00	186,66	1,93	1,381	1.00	182
KCIPHER	131,29	11,061	3,3258	1.00	186,71	0,489	0,699	1,00	186
MICKEY_2	133,53	61,65	7,85	1,00	186,6	2,302	1,51	1,00	179
MUGI	132,23	53,721	7,329	1.00	186,5	0,978	0,989	1.00	185
RABBIT	132,65	16,87	4,017	1,00	187,22	0,451	0,657	1,00	185
RC4	133,7	67,01	8,186	1,00	186,3	1,61	1,269	1,00	184
SALSA20	134,16	28,055	5,27	1,00	187,001	1,01	0,99	1,00	183
SNOW2.0	132.78	23.93	4.89	1.00	186.79	0.43	0.656	1.00	183
SOSEMANUK	131,73	49,36	6,991	1,00	186,8	2,240	1,49	1,00	184
STRUMOK_256	130,01	23,6	4,86	1.00	186,45	1,4555	1,206	1.00	184
STRUMOK 512	132,83	56,516	7,518	1.00	186,90	0,802	0,896	1.00	185
TRIVIUM	130,24	99,683	9,935	1,00	187,15	1,49	1,214	1,00	182

В табл. 2 наведено такі дані:

– «M096» та «M099» – оцінки математичного сподівання (вибіркові середні) числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ та за критерієм $P_j \geq 0{,}99$, відповідно;

– «D096» та «D099» («S096» та «S099») – оцінки дисперсії (середньоквадратичних відхилень) результатів тестування числа пройдених статистичних тестів за критеріями $P_j \geq 0{,}96$ та $P_j \geq 0{,}99$, відповідно;

– «P099» – значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}99$ та при точності $\varepsilon = 2$;

– «P096» – значення довірчої ймовірності для числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ та при точності $\varepsilon = 1$;

– «Min096» мінімальні значення числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$.

Наведені результати тестування різних шифрів підтверджують їх високі криптографічні властивості. Зокрема, всі досліджувані криптоперетворення показали високе число успішно пройдених тестів: 130 – 134 за критерієм $P_j \geq 0{,}99$ та 186 – 187 за критерієм $P_j \geq 0{,}96$ (окрім CryptMT, який отримав результат 158). Ці оцінки отримано з дуже високою достовірністю, наприклад, $P_o = 0{,}99$ для критерію $P_j \geq 0{,}99$ та $P_o \approx 1$ для критерію $P_j \geq 0{,}96$. Мінімальні

значення числа пройдених статистичних тестів коливаються від 179 до 186 тестів. Найбільше число пройдених тестів показав KCipher.

Слід відмітити високі показники статистичної безпеки алгоритму ПСШ «Струмок», який виявив певні властивості генератору випадкових бітів. Зокрема за результатами даних табл. 2 видно, що формовані ПВП за своїми властивостями не поступаються ПВП, які сформовано всесвітньо відомими потоковими криптографічними алгоритмами, зокрема шифрами HC-256 та SNOW 2.0. Крім того, для ПСШ «Струмок» мінімальні значення числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ є вищі ніж у цих алгоритмах, що свідчить про незначну перевагу показників статистичної безпеки алгоритму.

Набір статистичних тестів DIEHARD запропоновано у 1995 році Джорджем Марсальгія [21]. DIEHARD розглядаються як набір тестів з найбільш суворими критеріями до властивостей послідовності. Тести DIEHARD мають на меті характеризувати випадковість (або її відсутність) в послідовності цілих чисел, сформованих певним генератором псевдовипадкових послідовностей.

Специфічною властивістю системи DIEHARD є практична спрямованість тестів, тобто в основі деяких тестів лежать не теоретичні розрахунки оцінки статистичної безпеки, а оцінка результатів на основі проведених раніше автором практичних випробувань. Завдяки специфічній побудові цей пакет відрізняється тим, що для нього важко сформувати погану послідовність, яка не задовольняє вимогам випадковості, проте успішно б пройшла усі тести.

До складу DIEHARD входить 12 алгоритмів тестування:

1) *Дні народження (Birthday Spacings).* Обираються випадкові точки на великому інтервалі. Відстані між точками повинні бути асимптотично розподілені за Пуассоном. Назву цей тест отримав на основі парадоксу днів народження.

2) *Перестановки, що пересікаються (Overlapping Permutations).* Аналізуються послідовності п'яти послідовних випадкових чисел. 120 можливих перестановок повинні зустрічатися зі статистично еквівалентної ймовірністю.

3) *Тести бітового потоку (Monkey Tests, Bitstream test).* Послідовності з деякої кількості біт інтерпретуються як слова. Вважаються слова, що пересікаються, в потоці. Кількість «слів», які не з'являються, повинні задовольняти відомому розподілу. Назву цей тест отримав на основі теореми про нескінченну кількість мавп.

4) *Ранги матриць (Ranks of matrices).* Обираються кілька біт з деякої кількості випадкових чисел для формування матриці над {0,1}, потім визначається ранг матриці.

5) *Підрахунок одиниць (Count the 1's).* Підраховуються поодинокі біти в кожному з наступних або обраних байт.

6) *Тест на парковку (Parking Lot Test).* Одиничні окружності випадково розміщуються в квадраті 100 × 100. Якщо окружність перетинає вже існуючу, робиться спроба повторного розміщення окружності. Після 12 000 спроб, кількість успішно «припаркованих» кіл повинна бути нормально розподілена.

7) *Тест на мінімальну відстань (Minimum Distance Test).* 8000 точок випадково розміщуються в квадраті 10 000 × 10 000, потім знаходиться мінімальна відстань між будь-якими парами. Квадрат цієї відстані повинен бути експоненційно розподілений з деякою медіаною.

8) *Тест випадкових сфер (Random Spheres Test).* Випадково вибираються 4000 точок в кубі з ребром 1000. У кожній точці поміщається сфера, чий радіус є мінімальною відстанню до іншої точки. Мінімальний об`єм сфери повинен бути експоненційно розподілений з деякою медіаною.

9) *Тест стиснення (The Squeeze Test).* 2^{31} множиться на випадкові дійсні числа в діапазоні [0,1) до тих пір, доки не вийде 1. Повторюється 100 000 раз. Кількість дійсних чисел необхідних для досягнення 1 повинна бути розподілена певним чином.

10) *Тест сум, що пересікаються (Overlapping Sums Test).* Генерується довга послідовність дійсних чисел з інтервалу [0,1). У ній підсумовуються кожні 100 послідовних чисел. Суми повинні бути нормально розподілені з характерними середнім і дисперсією.

11) *Тест послідовностей (Runs Test).* Генерується довга послідовність на інтервалі [0,1). Підраховуються висхідні і низхідні послідовності. Числа повинні задовольняти деякого розподілу.

12) *Тест гри в кості (The Craps Test).* Граються 200 000 ігор в кістки, підраховуються перемоги і кількість кидків в кожній грі. Кожне отримане число має задовольняти деякому розподілу.

До складу програмної реалізації DIEHARD в залежності від вхідних даних загалом входить 215 тестів. Для оцінки результатів їх проходження використовують сукупну оцінку ймовірності з використанням критерію Колмогорова – Смирнова (KS), тобто значення декількох P_j згортаються на остаточну оцінку, використовуючи KS-тести. Критерій KS може використовуватися в тому випадку, коли результати випробувань становлять нескінчену множину. Його сутність полягає в наступному. Нехай у результаті n випробувань були отримані значення $X_i, i=\overline{1,n}$. Побудуємо емпіричну функцію розподілу

$$F_n(x)=\frac{1}{n}\sum_{i=1}^{n} X_i \le x .$$

Критерій KS визначає, наскільки емпірична функція розподілу $F_n(x)$ відрізняється від функції розподілу $F(x)$, яка визначає ймовірність того, що випадкова величина X матиме значення, менше або рівне x для заданого розподілу. Однак розрахунки цього критерію досить трудомісткі, тому замість критерію KS у математичній статистиці використовується критерій Андерсона – Дарлінга.

За критерієм Андерсона – Дарлінга приймається, що було проведено n випробувань й отримано статистики $X_i, i=\overline{1,n}$. В тесті DIEHARD результатом проведення тесту є ймовірність P_j. Якщо розташувати ці величини за зростанням, отримаємо

$$P_1 \le P_2 \le P_3 \le \ldots \le P_n .$$

В такому випадку тестова статистика приймає значення

$$A^2 = -n - \sum_{j=1}^{n} \frac{2j-1}{n}\left[\ln P_j + \ln P_{n+1-j}\right].$$

Остаточна оцінка ймовірності визначається як

$$P_{jKS}=\begin{cases} 0, & A^2 < \alpha \\ 2e^{-\frac{1.2337}{A^2}}\left(1+\frac{A^2}{2^3}-\frac{0.04958\left(A^2\right)^2}{1.325+A^2}\right), & \alpha \le A^2 < 2 \\ 1-0.6621361\cdot e^{-1.091638\cdot A^2}-0.95095\cdot e^{-2.005138\cdot A^2}, & 2 \le A^2 < 4 \\ 1-0.4938691\cdot e^{-1.050321\cdot A^2}-0.5946336\cdot e^{-1.527198\cdot A^2} & A^2 \ge 4 \end{cases},$$

де α – рівень значущості.

Таким чином, для оцінки проходження певного *j*-тесту використовуються значення ймовірності P_j або ймовірність отримана за критерієм Андерсона – Дарлінга P_{jKS}.

Відомо, що при тестуванні статистичних властивостей дійсно випадкової послідовності характерною властивістю є рівномірний розподіл отриманих ймовірностей проходження тестів. Тобто, серед усіх отриманих значень ймовірностей P_j їх розподіл має бути рівномірним на одиничному інтервалі. Відхилення від рівномірного розподілу вказують на те, що деякі з тестів DIEHARD виявили впорядковані шаблони у послідовності, що тестується. Якщо отримані 215 значень ймовірностей P_j, впорядковані за зростанням, представити у вигляді графіку, можна наочно визначити будь-які, навіть незначні, відхилення від рівномірного розподілу. Приклад результатів тестування «поганої», в статистичному сенсі, послідовності наведено на рис. 1. Ця послідовність була сформована стандартним генератором випадкових чисел для мови C++. З розподілу зрозуміло, що відповідний генератор не може використовуватися в якості частини реалізації криптографічного алгоритму шифрування.

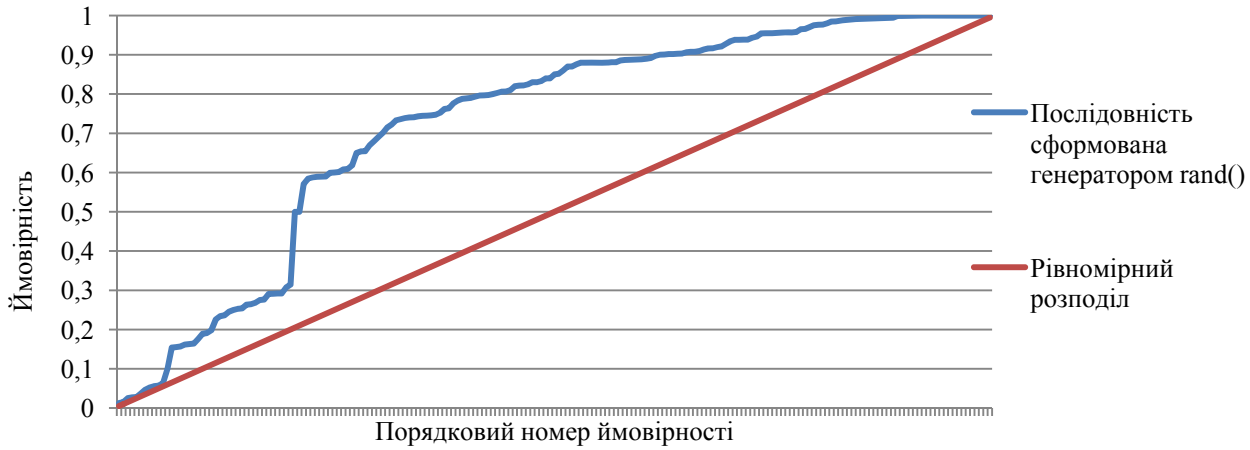


Рис. 1. Розподіли ймовірностей «поганої» послідовності

Результати статистичного тестування пакетом DIEHARD для симетричних шифрів AES, CryptMT, DECIM, Enocoro, Grain, HC, KCipher, Mickey2, MUGI, Rabbit, RC4, Salsa20, Snow 2, Sosemanuk, Trivium та ПСШ «Струмок» у вигляді розподілів ймовірностей на одиничному інтервалі наведено на рис. 2 – 19. На рис. 20 – 37 зображено статистичні портрети результатів тестування пакетом DIEHARD для симетричних шифрів.

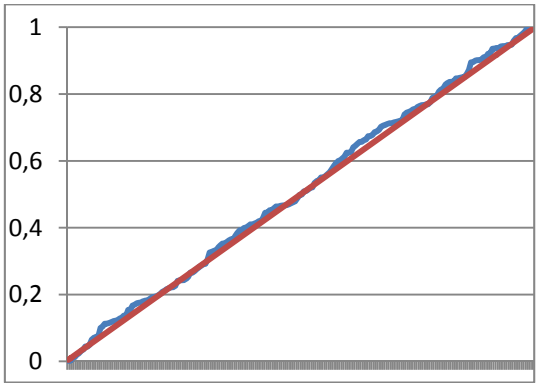


Рис. 2. AES-128

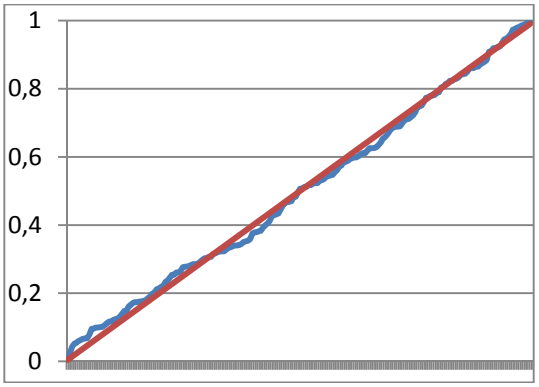


Рис. 3. AES-256

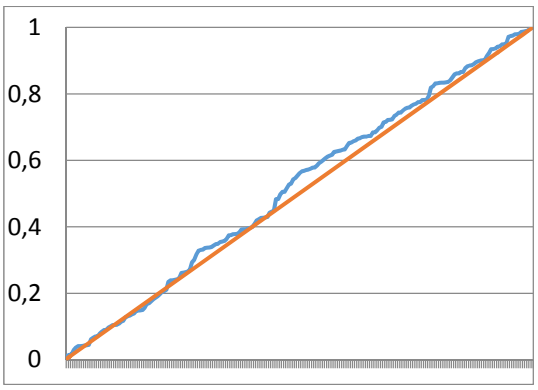


Рис. 4. CryptMT

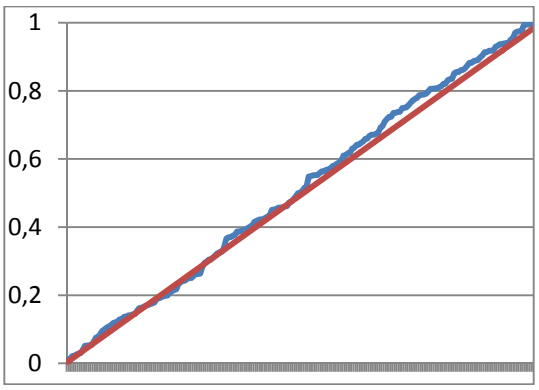


Рис. 8. HC-128

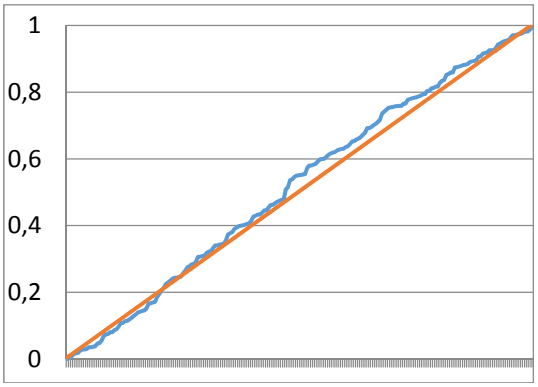


Рис. 5. DECIM

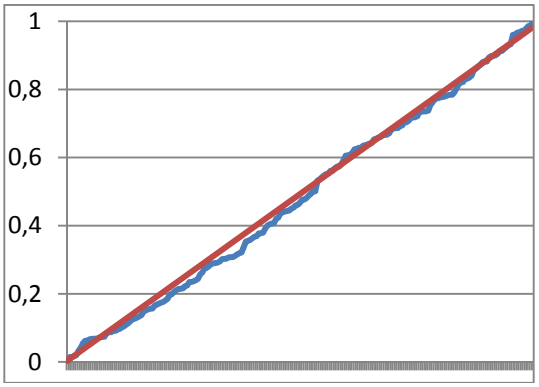


Рис. 9. HC-256

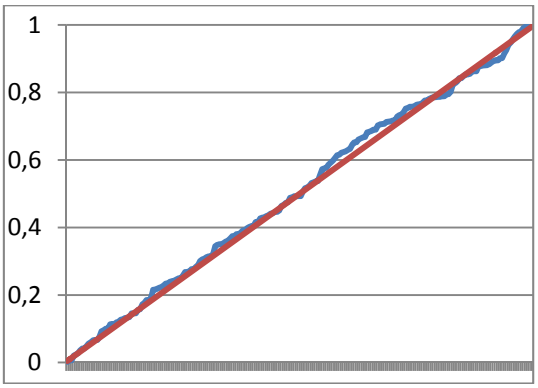


Рис. 6. Enocoro

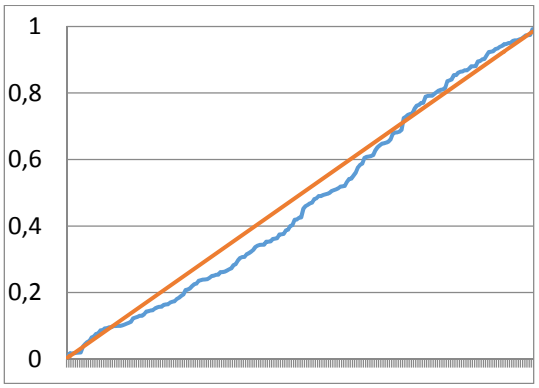


Рис. 10. KCipher

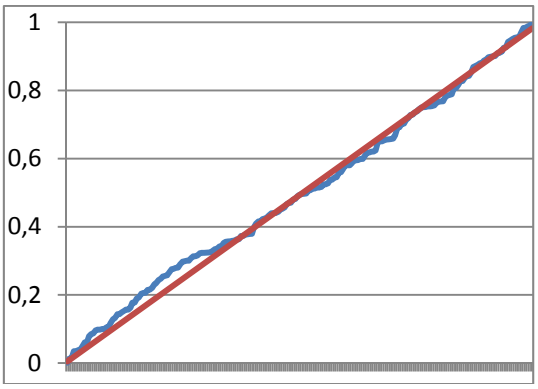


Рис. 7. Grain

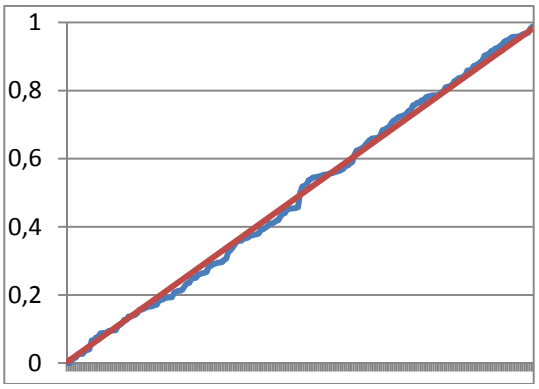


Рис. 11. Mickey2

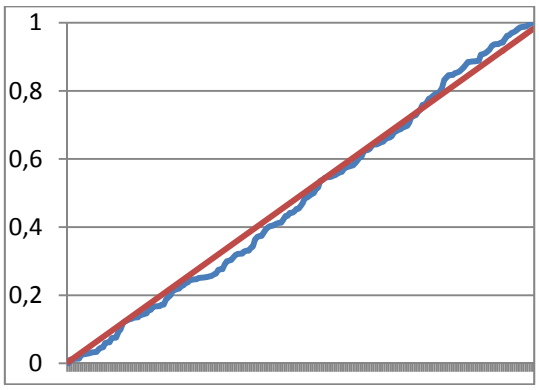


Рис. 12. MUGI

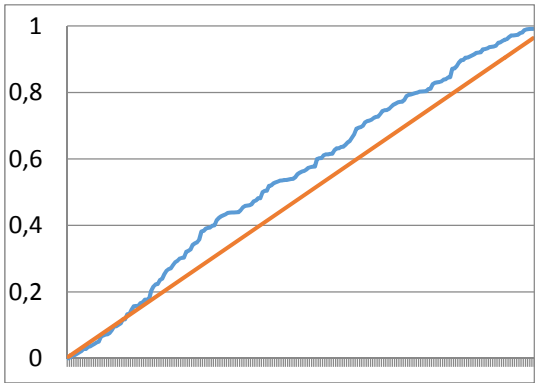


Рис. 13. RC4

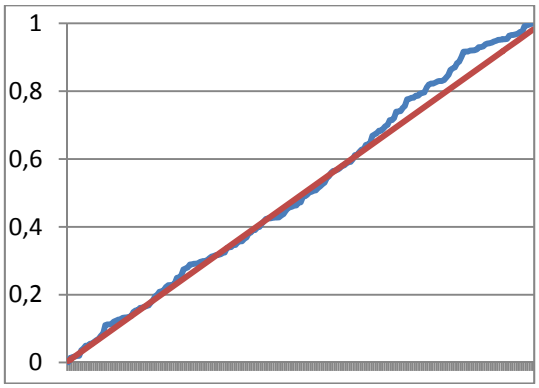


Рис. 14. Salsa20

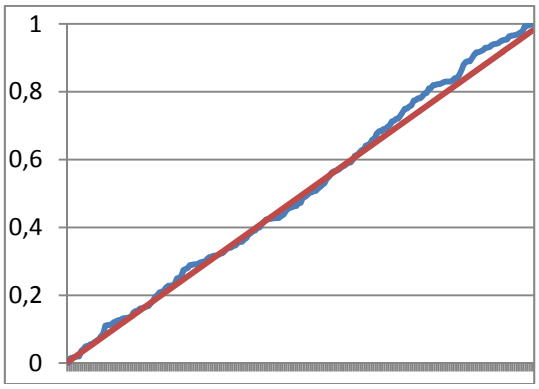


Рис. 15. Snow 2

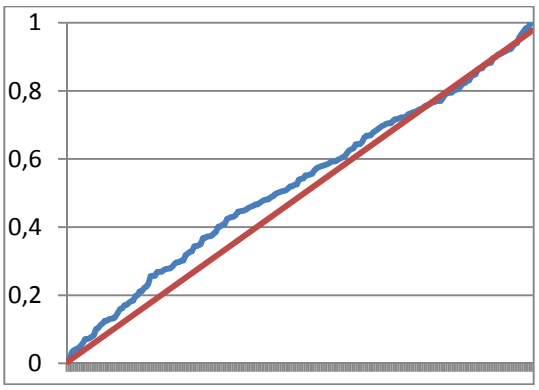


Рис. 16. Sosemanuk

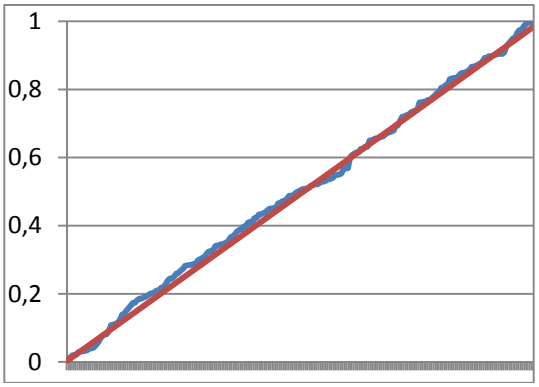


Рис. 17. «Струмок-256»

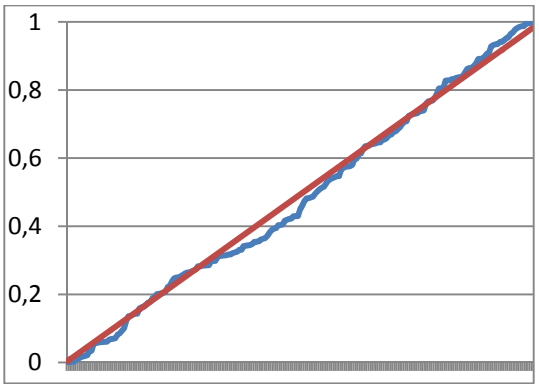


Рис. 18. «Струмок-512»

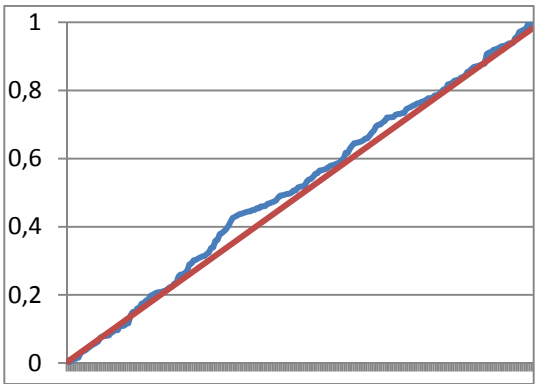


Рис. 19. Trivium

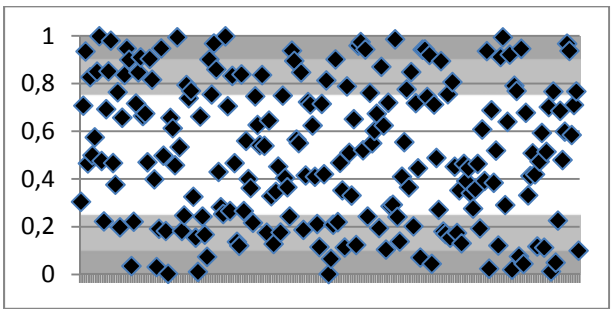


Рис. 20. AES-128

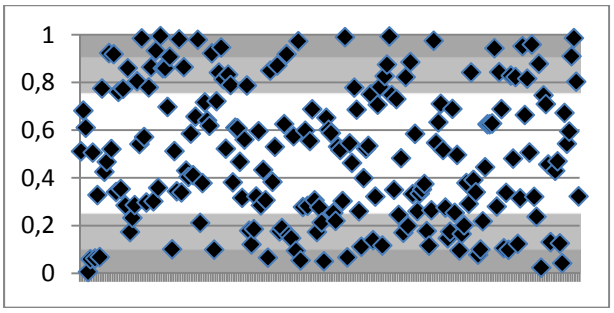


Рис. 21. AES-256

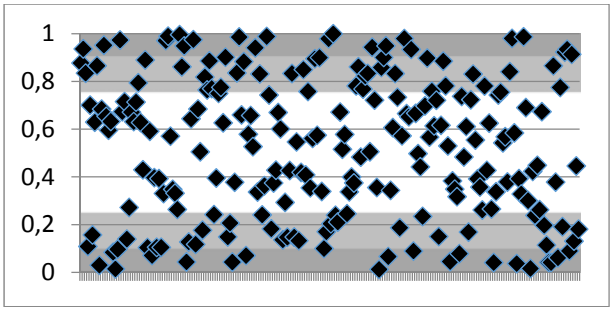


Рис. 22. CryptMT

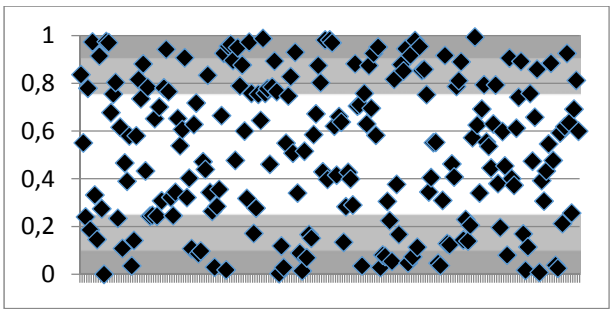


Рис. 23. DECIM

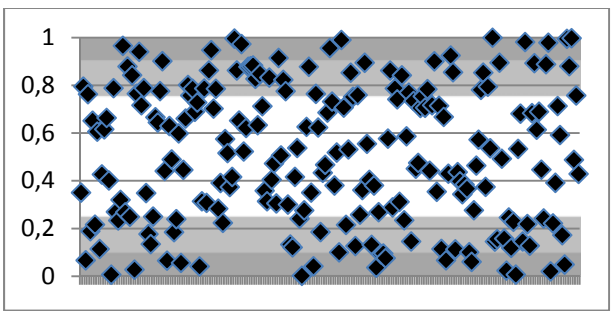


Рис. 24. Enocoro

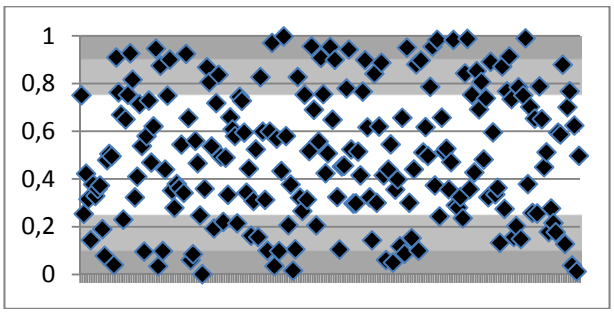


Рис. 25. Grain

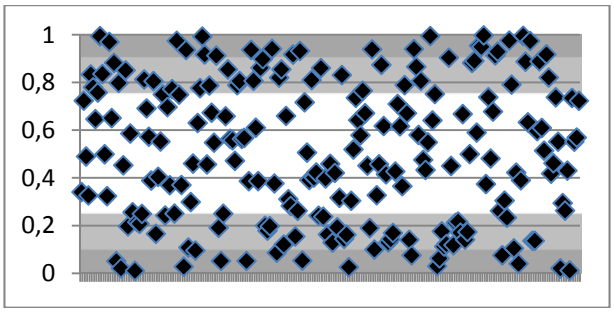


Рис. 26. HC-128

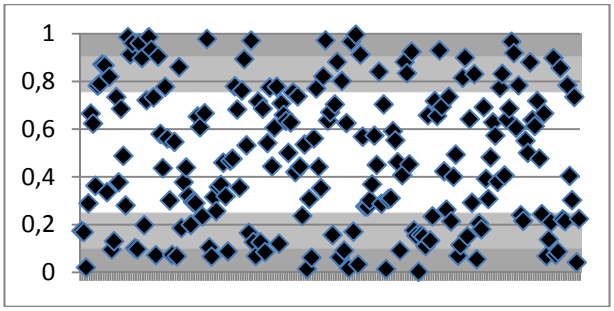


Рис. 27. HC-256

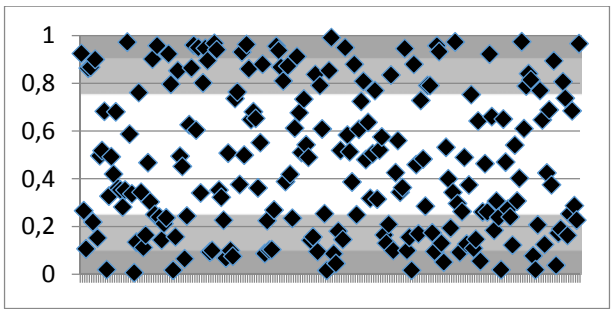


Рис. 28. KCipher

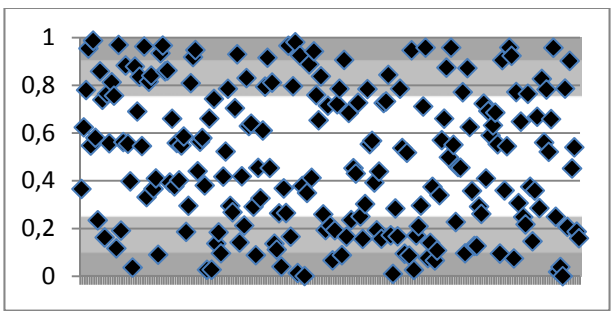


Рис. 29. Mickey2

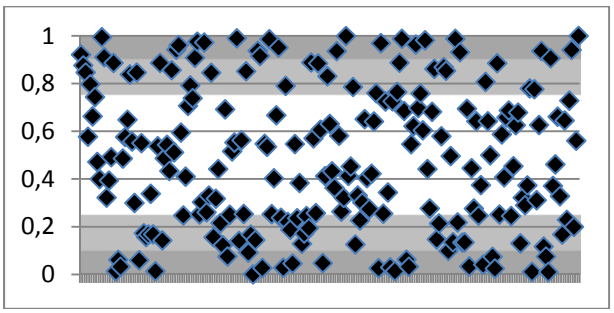


Рис. 30. MUGI

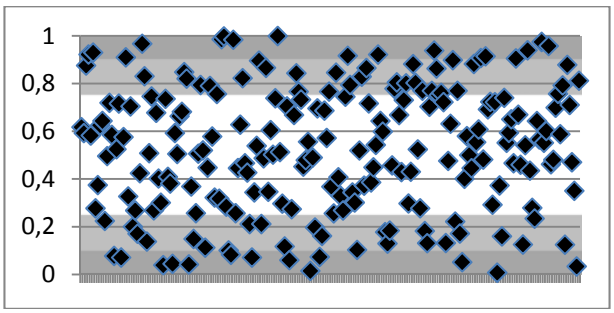


Рис. 34. Sosemanuk

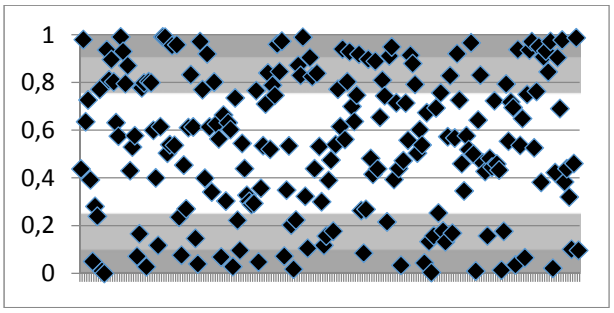


Рис. 31. RC4

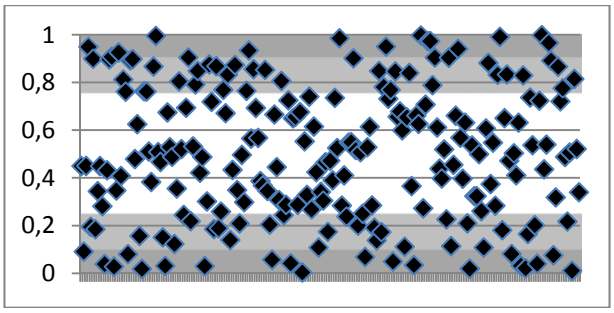


Рис. 35. «Струмок-256»

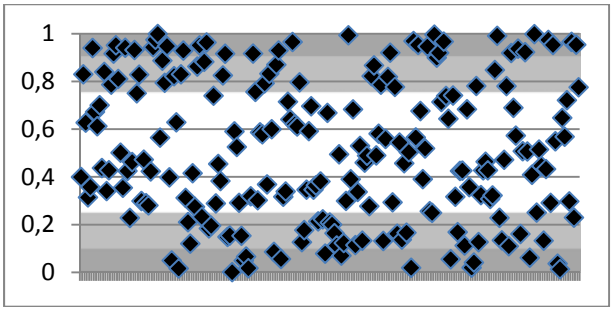


Рис. 32. Salsa20

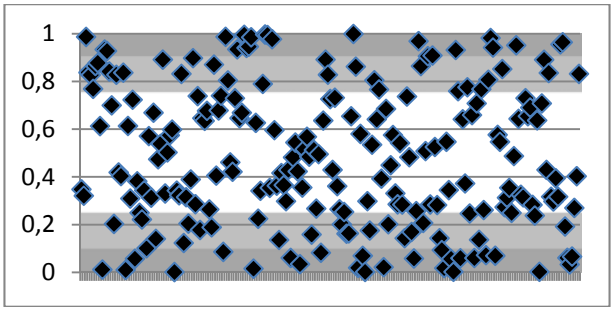


Рис. 36. «Струмок-512»

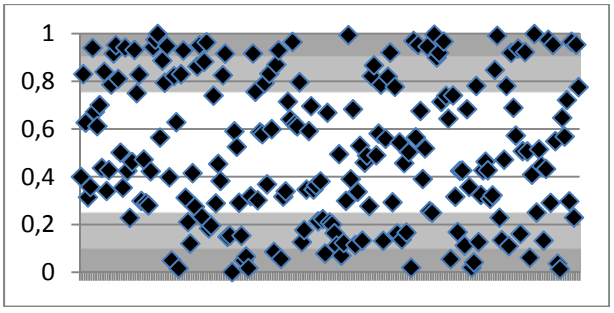


Рис. 33. Snow 2

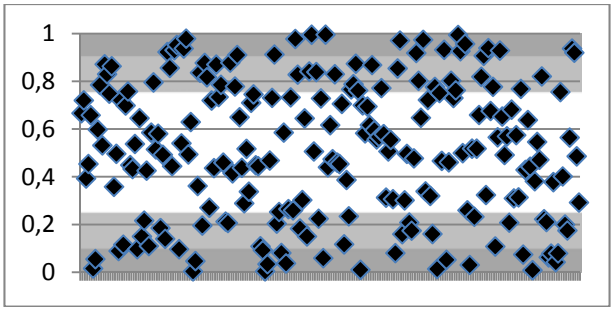


Рис. 37. Trivium

Розподіл ймовірностей на одиничному інтервалі дає можливість приблизно оцінити випадковість послідовності, що була протестована, на відповідність до розподілу дійсно випадкової послідовності. Можна побачити, що розподіл ймовірностей для більшості шифрів відповідає рівномірному розподілу з невеликими флуктуаціями.

Для оцінки статистичних властивостей за результатами проходження тестів в [22] використовується дещо інший підхід. Умовно розділимо одиничний відрізок на декілька підінтервалів. Якщо ймовірність належить певному інтервалу це характеризує проходження j-го тесту як:

1) провал тесту, при ймовірності $P_j \le 0.1$ або $P_j > 0.9$
2) результати тесту сумнівні, якщо ймовірність належить до одного із під інтервалів $0.1 < P_j \le 0.25$ або $0.75 < P_j \le 0.9$;
3) тест пройдено, якщо ймовірність приймає значення $0.25 < P_j \le 0.75$.

Очевидно, що у випадку, коли більшість результатів належить інтервалу (0.25,0.75] можна вважати, що послідовність має достатні статистичні властивості у порівнянні з дійсно випадковою. Якщо переважна більшість результатів належить інтервалам (0,0.25) та [0.9,1) послідовність, що тестується можна вважати поганою в статистичному сенсі.

Підрахована кількість ймовірностей проходження тестів для кожного з зазначених шифрів зведена до табл. 3.

Таблиця 3

Кількість результатів проходження тестів розподілених за п'ятьма інтервалами

Ймовірність / Шифр	$P_j \le 0.1$	$0.1 < P_j \le 0.25$	$0.25 < P_j \le 0.75$	$0.75 < P_j \le 0.9$	$P_j > 0.9$
AES-128	16	37	109	28	25
AES-256	15	33	115	31	21
CRYPTMT	21	34	99	36	25
DECIM	25	29	93	42	26
ENOCORO	18	36	102	43	16
GRAIN	17	26	122	31	19
HC-128	17	37	103	36	22
HC-256	25	33	109	30	18
KCIPHER-2	25	41	90	39	20
MICKEY2	21	35	104	32	23
MUGI	25	33	107	27	23
RC4	23	21	104	35	32
SASLA20	17	33	106	27	32
SNOW 2.0	21	31	112	33	18
SOSEMANUK	13	25	126	34	17
STRUMOK 256	20	29	113	35	18
STRUMOK 512	26	26	113	28	22
TRIVIUM	24	27	107	35	22

Усі шифри показали достатній рівень статистичної безпеки. Для наочності кількість тестів, які пройдено, тобто у яких результат належить до інтервалу $0.25 < P_j \le 0.75$, зведено до гістограми на рис. 38.

Не дивлячись на те, що шифр Sosemanuk за результатами відповідності розподілу ймовірностей до рівномірного показав незначні, але дещо більші на відміну від інших шифрів, відхилення від рівномірного розподілу, за результатами останнього тесту займає провідну позицію. Також слід відмітити, що за кількістю пройдених статистичних тестів пакету NIST STS шифр KCipher займав першу позицію, але у тестуванні DIEHARD він на останньому місці.

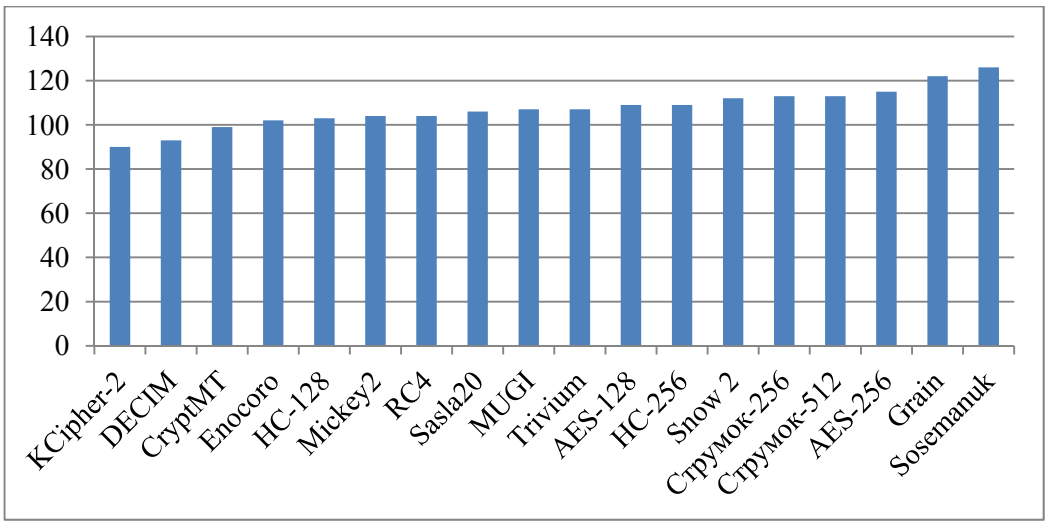


Рис. 38. Кількість успішно пройдених статистичних тестів DIEHARD

Порівняльні дослідження швидкодії алгоритмів потокового шифрування

Важливою характеристикою сучасних криптографічних засобів захисту інформації є показники швидкодії, які характеризують здатність криптосистеми обробляти великі обсяги даних за встановлений час. В цьому розумінні важливим є дослідження швидкісних характеристик потокових шифрів, їх порівняння за різними критеріями, які відображають здатність криптопримітивів до швидкої обробки різних за обсягами масивів даних [1 – 5, 11].

В цій роботі аналіз швидкодії потокових шифрів проводиться за методикою, яка була запропонована на всесвітньовідомому конкурсі eSTREAM [8]. Ця методика полягає у тестуванні за різними реальними ситуаціями, які можуть виникати у каналах передачі інформації, передбачено наступні критерії:

1. Критерій зашифрування довгих потоків. Поточні шифри мають найбільш потенційну перевагу над блочними шифрами при зашифруванні довгих потоків;
2. Критерій зашифрування коротких потоків. Цей показник відображає швидкість зашифрування пакетів різної (зазвичай, невеликої) довжини;
3. Критерій ініціалізації/генерації ключових параметрів. Ця характеристика окремо відображає ефективність встановлення ключа та вектору ініціалізації.

Усі шифри були реалізовані за допомогою ЕОМ з процесором Intel(R) Pentium(R) CPU P6200 @ 2.13GHz, 2128, RAM: 2 по 2 ГБ(з частотою 1333МГц), КЕШ: 1-го рівня (128 Кб); 2-го рівня (512 Кб); 3-го рівня (3072 Кб) в операційній системі Windows 8.1 Професійна 64bit, на компіляторі Microsoft Visual Studio 2012 32bit версії 11.00.50727.1.

Після реалізації обраних шифрів усі шифри були запущені на різних за потужністю/продуктивністю процесорах, на різних платформах, реалізованих на різних мовах програмування та компіляторах. Результати тестування представлено нижче.

Тестування за критерієм швидкості зашифрування довгих потоків. Однією з областей, де можуть використовуватися поточні шифри, є шифрування довгих потоків. Ця задача виникає при шифруванні даних об’ємних носіїв інформації, зокрема жорсткого диску [8]. Наприклад, для забезпечення конфіденційності особистих даних користувачі можуть шифрувати носії інформації, але платою за це є зниження швидкості роботи операційної системи.

Для визначення показників швидкості сучасних шифрів проведено експериментальні дослідження, в яких використано програмне забезпечення VeraCrypt та TrueCrypt для шифрування дискового простору [23, 24]; виконано стандартні тести перевірки швидкості шифрування для усіх можливих реалізованих алгоритмів. Експеримент проводився у наступних умовах: згенерували об’єм даних у розмірі 1 Гб та шифри: AES, Twofish, AES-

Twofish, SERPENT, SERPENT-AES, AES-Twofish-SERPENT, SERPENT-Twofish-AES, Twofish-SERPENT, зашифровували та розшифровували дані. Отримані експериментальні результати продемонстровано на рис. 39 та 40.

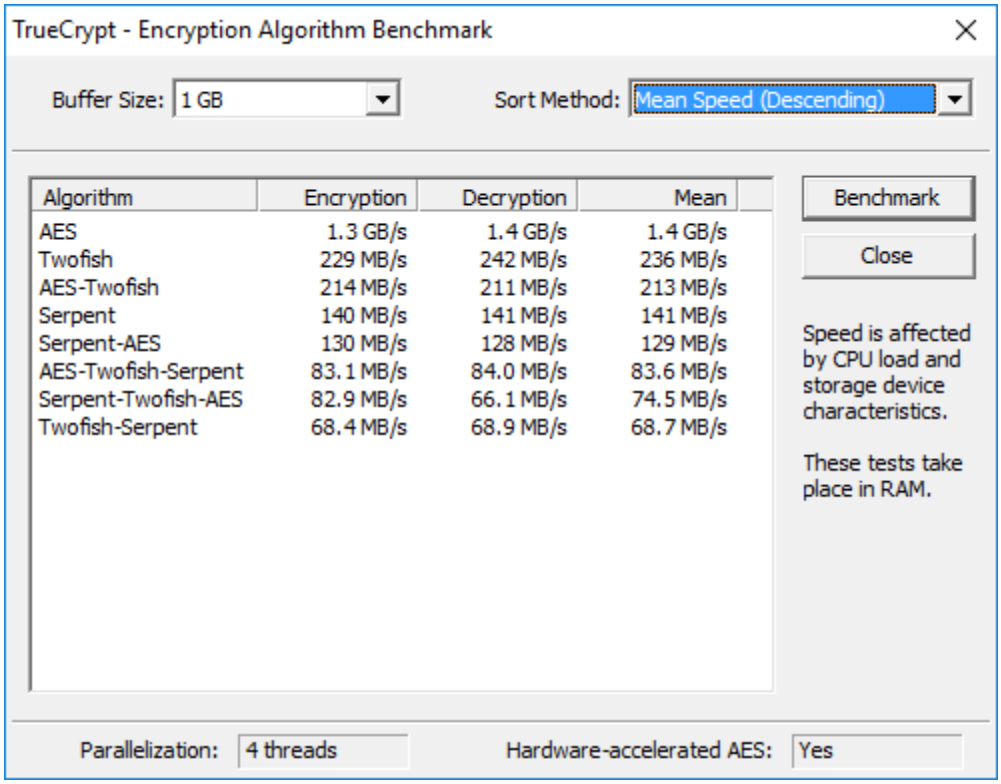


Рис. 39. Результати експериментальних досліджень за допомогою TrueCrypt

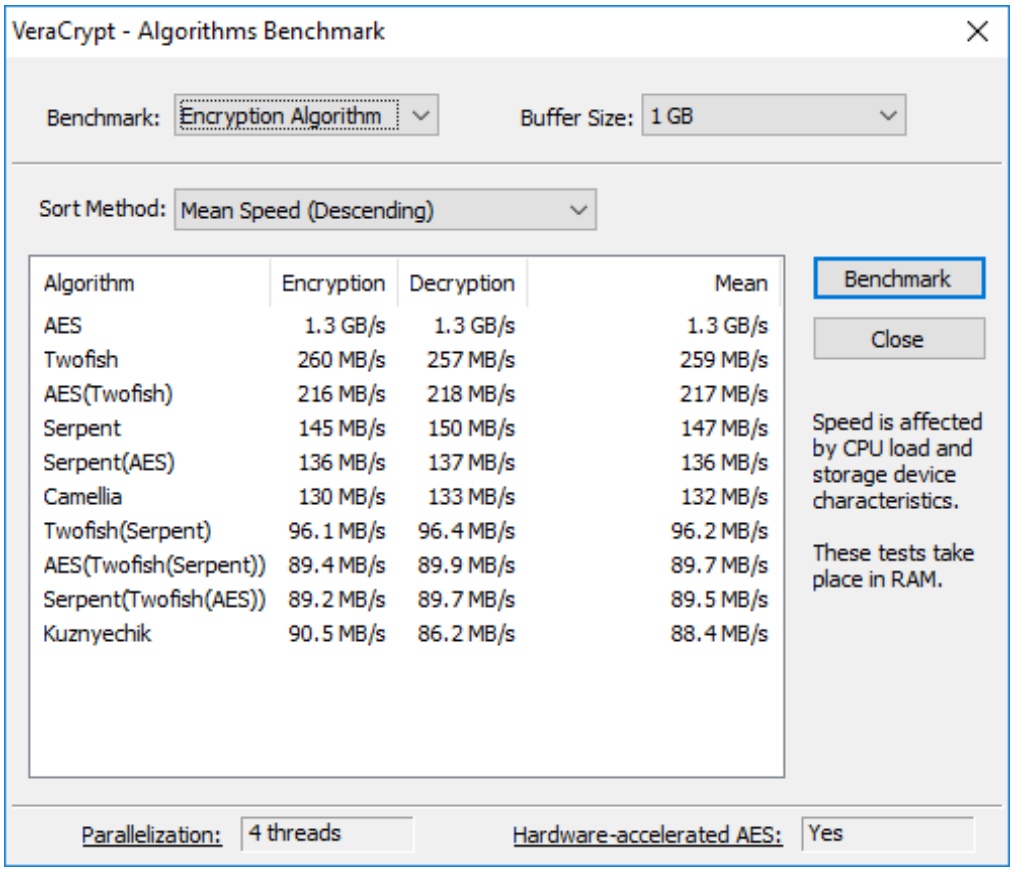


Рис. 40. Результати експериментальних досліджень за допомогою VeraCrypt

Критерій шифрування довгих потоків характерний саме для потокових шифрів, тому увага до цих показників приділяється в першу чергу. За методикою дослідження випадковим чином генеруються дані об'ємом у 1 Гб, потім випадково генерується один ключ та за допомогою вектору ініціалізації встановлюється випадковий стан регістрів. Наступним кроком відбувається безпосередньо шифрування 1 Гб даних, та вимірюється час протікання процесу шифрування і пропускна здатність алгоритму (кількість байт, зашифрованих за одну мікросекунду). Результати зібрані у табл. 4. Найкращі показники за критерієм шифрування довгих повідомлень показали «Струмок», HC-128 та "SNOW 2.0".

Таблиця 4

Результати експериментальних досліджень швидкісних характеристик шифрів на різних за потужністю процесорах

Назва шифру	Зашифрування 1GB (Intel Core i7-6820HQ 2.7Gh)		Зашифрування 1GB (Intel Core i7-5500u 2.4Gh)		Зашифрування 1GB (Intel Pentium P6200 2.13Gh)	
	Час, ms	Швидкість, bytes / µs	Час, ms	Швидкість, bytes / µs	Час, ms	Швидкість, bytes / µs
AES-128	3229	332,51	4570	234,97	9787	109,72
AES-256	4819	236,83	6766	158,69	14133	75,98
HC-128	698	1537,65	1040	1032,25	2073	518,09
HC-256	1559	688,83	2061	521,08	4465	240,47
MICKEY-128	116786	9,19	164304	6,54	265471	4,05
RABBIT	2190	490,27	2893	371,22	5656	189,85
SALSA-20	2650	405,26	3885	276,40	8428	127,40
SNOW2.0-128	913	1176,19	1474	728,50	2924	367,18
SNOW2.0-256	917	1170,80	1445	742,87	2989	359,22
SOSEMANUK	1967	545,82	3124	343,69	4973	215,91
STRUMOK 256	601	1788,08	797	1347,06	3648	294,33
STRUMOK 512	584	1839,54	821	1308,01	3677	292,03
TRIVIUM	2058	521,72	2879	372,93	5016	214,05
CryptMT3	1351	794,83	1728	621.378370	1981	541,97
DECIM-128	703486	1,53	815187	1,32	994679	1,08
RC4	2232	481,07	2491	431,05	4786	224,35
KCIPHER-2	20253	53,02	20253	53,02	25986	41,32
GRAIN	1263313	0,85	1456900	0,74	1864210	0,58
MUGI	2207	486,45	2685	399,95	3098	346,57

Беручу до уваги результати експериментальних досліджень швидкісних характеристик шифрів на різних за потужністю процесорах, можна побачити, що на процесорах з невеликою частотою шифр «Струмок» програє у швидкості, але на більш потужних процесорах швидкість зростає. Цей програш, насамперед, обумовлений більшим розміром блоку ніж у інших алгоритмів, на який витрачається більше часу обчислення процесором математичних операцій.

Тестування за критерієм швидкості зашифрування коротких потоків. Швидкість зашифрування довгих потоків є основною характеристикою блокових шифрів, яка відображає спроможність криптопримітиву функціонувати за своїм цільовим призначенням. Тому при тестуванні потокових шифрів цей критерій досліджується для визначення

поведінки структури алгоритмів, визначення слабких сторін та виявлення переваг і недоліків певних шифрів.

Критерій зашифрування коротких потоків відповідно до методики дослідження відображає швидкість зашифрування пакетів різної довжини (40 байт, 576 байт та 1500 байт), які репрезентовано відображають трафік телекомунікаційного каналу передачі інформації. Тобто ці дослідження є певною імітацією функціонування потокового шифру при його використанні для шифрування трафіку сучасних телекомунікаційних систем із комутацією пакетів.

Відповідно до методики дані пакетів генеруються випадковим чином. При тестуванні вимірюється час шифрування пакетів, швидкість зашифрованих байт на мікросекунду та швидкість зашифрованих пакетів на мікросекунду.

Результати тестування за критерієм шифрування коротких повідомлень зведено у табл. 5 – 7.

За узагальненням цих даних можна зробити наступні висновки:

– найкращі показники за критерієм зашифрування коротких потоків отримано для шифрів «Струмок», «SNOW 2.0» та «SOSEMANUK» відповідно;

– отримані показники демонструють те, що шифри «SNOW 2.0» та «SOSEMANUK» показують кращі показники у випадку, коли пакетів багато але малих за розміром даних;

– щодо потокового шифру «Струмок» маємо зворотні результати: шифр демонструє кращі показники, коли пакетів мало, але вони великі за розміром.

Таблиця 5

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Core i7-6820HQ 2.7Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs
AES-128	230	326,09	0,2174	211	327,58	0,5687	60	233,33	5,8333
AES-256	323	232,20	0,1548	300	230,40	0,4000	81	172,84	4,3210
HC-128	257	291,83	0,1946	546	126,59	0,2198	1492	9,38	0,2346
HC-256	1420	52,82	0,0352	3413	20,25	0,0352	9605	1,46	0,0364
MICKEY-128	7819	9,59	0,0064	7542	9,16	0,0159	3532	3,96	0,0991
RABBIT	154	487,01	0,3247	158	437,47	0,7595	88	159,09	3,9773
SALSA-20	190	394,74	0,2632	175	394,97	0,6857	58	241,38	6,0345
SNOW2.0-128	70	1071,43	0,7143	71	973,52	1,6901	64	218,75	5,4688
SNOW2.0-256	71	1056,34	0,7042	71	973,52	1,6901	64	218,75	5,4688
SOSEMANUK	91	824,18	0,5495	102	677,65	1,1765	79	177,22	4,4304
STRUMOK 256	49	1530,61	1,0204	60	1152,00	2,0000	76	184,21	4,6053
STRUMOK 512	50	1500,00	1,0000	61	1133,11	1,9672	75	186,67	4,6667
TRIVIUM	153	490,20	0,3268	168	411,43	0,7143	128	109,38	2,7344
CryptMT3	120	625,00	0,4167	183	377,70	0,6557	227	61,67	1,5419
DECIM-128	50291	1,49	0,0010	46635	1,48	0,0026	13122	1,07	0,0267
RC4	155	483,87	0,3226	149	463,89	0,8054	38	368,42	9,2105
KCIPHER-2	680	110,29	0,0735	1063	65,02	0,1129	745	18,79	0,4698
GRAIN	108503	0,69	0,0005	1000586	0,07	0,0001	34241	0,41	0,0102
MUGI	177	423,73	0,2825	205	337,17	0,5854	212	66,04	1,6509

Таблиця 6

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Core i7-5500u 2.4Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs	Час, µs	Швидкість, bytes / µs	Швидкість, packets / µs
AES-128	313	239,62	0,1597	291	237,53	0,4124	91	153,85	3,8462
AES-256	432	173,61	0,1157	406	170,25	0,2956	113	123,89	3,0973
HC-128	412	182,04	0,1214	844	81,90	0,1422	2241	6,25	0,1562
HC-256	2148	34,92	0,0233	4916	14,06	0,0244	14225	0,98	0,0246
MICKEY-128	10651	7,04	0,0047	10462	6,61	0,0115	4963	2,82	0,0705
RABBIT	210	357,14	0,2381	209	330,72	0,5742	105	133,33	3,3333
SALSA-20	262	286,26	0,1908	233	296,65	0,5150	77	181,82	4,5455
SNOW2.0-128	118	635,59	0,4237	117	590,77	1,0256	101	138,61	3,4653
SNOW2.0-256	110	681,82	0,4545	120	576,00	1,0000	103	135,92	3,3981
SOSEMANUK	150	500,00	0,3333	171	404,21	0,7018	122	114,75	2,8689
STRUMOK 256	66	1136,36	0,7576	82	842,93	1,4634	108	129,63	3,2407
STRUMOK 512	69	1086,96	0,7246	84	822,86	1,4286	126	111,11	2,7778
TRIVIUM	211	355,45	0,2370	238	290,42	0,5042	175	80,00	2,0000
CryptMT3	155	483,87	0,3226	229	301,83	0,5240	277	50,54	1,2635
DECIM-128	56987	1,32	0,0009	53800	1,28	0,0022	15067	0,93	0,0232
RC4	174	431,03	0,2874	172	401,86	0,6977	41	341,46	8,5366
KCIPHER-2	680	110,29	0,0735	1063	65,02	0,1129	745	18,79	0,4698
GRAIN	110360	0,68	0,0005	85329	0,81	0,0014	29499	0,47	0,0119
MUGI	225	333,33	0,2222	255	271,06	0,4706	248	56,45	1,4113

Таблиця 7

Експериментальні результати дослідження за критерієм шифрування коротких повідомлень (Intel Pentium P6200 2.13Gh)

Назва шифру	Зашифрування пакетів								
	50 пакетів по 1500 байт			120 пакетів по 576 байт			350 пакетів по 40 байт		
	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs	Час, μs	Швидкість, bytes / μs	Швидкість, packets / μs
AES-128	383	195,82	0,1305	353	195,81	0,3399	100	140,00	3,5000
AES-256	538	139,41	0,0929	507	136,33	0,2367	141	99,29	2,4823
HC-128	452	165,93	0,1106	949	72,83	0,1264	2581	5,42	0,1356
HC-256	2530	29,64	0,0198	5769	11,98	0,0208	16320	0,86	0,0214
MICKEY-128	12803	5,86	0,0039	12625	5,47	0,0095	5923	2,36	0,0591
RABBIT	289	259,52	0,1730	284	243,38	0,4225	149	93,96	2,3490
SALSA-20	340	220,59	0,1471	313	220,83	0,3834	103	135,92	3,3981
SNOW2.0-128	124	604,84	0,4032	123	561,95	0,9756	117	119,66	2,9915
SNOW2.0-256	125	600,00	0,4000	141	490,21	0,8511	122	114,75	2,8689
SOSEMANUK	163	460,12	0,3067	183	377,70	0,6557	131	106,87	2,6718
STRUMOK 256	83	903,61	0,6024	103	671,07	1,1650	131	106,87	2,6718
STRUMOK 512	86	872,09	0,5814	104	664,62	1,1538	133	105,26	2,6316
TRIVIUM	275	272,73	0,1818	298	231,95	0,4027	227	61,67	1,5419
CryptMT3	180	416,67	0,2778	281	245,98	0,4270	369	37,94	0,9485
DECIM-128	71205	1,05	0,0007	67090	1,03	0,0018	19255	0,73	0,0182
RC4	333	225,23	0,1502	320	216,00	0,3750	78	179,49	4,4872
KCIPHER-2	971	77,24	0,0515	1409	49,06	0,0852	1028	13,62	0,3405
GRAIN	135271	0,55	0,0004	128127	0,54	0,0009	44250	0,32	0,0079
MUGI	253	296,44	0,1976	296	233,51	0,4054	317	44,16	1,1041

Тестування за критерієм швидкості ініціалізації/генерації ключових параметрів. Цей критерій окремо характеризує такий елемент структури шифрів, як встановлення ключа та вектору ініціалізації. Ці дві складові структури шифру є найменш критичні для відображання швидкості алгоритму, так як мало затрачується на встановлення ключа та вектору ініціалізації в порівнянні з процесом шифрування.

За методикою було визначено наступне: для оцінки схеми розгортання ключа потрібно зробити 7000 ключових установок, це 700 установок на один ключ (10 ключів на 700 установок). Для оцінки процесу ініціалізації початкового вектору визначено наступне: 500 ключових установок, це 50 установок на один вектор (10 векторів по 50 установок).

Для оцінки описаних параметрів буде фіксуватися загальний час виконання операції, кількість затрачених циклів на установку та кількість установок, яких можна зробити за одну секунду.

Отримані результати зведено у табл. 8 – 10.

Таблиця 8

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Core i7-6820HQ 2.7Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	483	14,5	0,09	5555,6
AES-256	1075	6,5	0,06	8333,3
HC-128	22	318,2	2101,6	0,2
HC-256	339	20,6	13347,6	0,0
MICKEY-128	7	1000,0	2987,8	0,2
RABBIT	886	7,9	58,3	8,6
SALSA-20	25	280,0	0,09	5555,6
SNOW2.0-128	33	212,1	54,9	9,1
SNOW2.0-256	64	109,4	55,1	9,1
SOSEMANUK	1084	6,5	70,2	7,1
STRUMOK 256	33	212,1	62,4	8,0
STRUMOK 512	34	205,9	61,3	8,2
TRIVIUM	46	152,2	138	3,6
CryptMT3	223	31,4	281,4	1,8
DECIM-128	2	3500,0	7889	0,1
RC4	5793	1,2	-	-
KCIPHER-2	182	38,5	751	0,7
GRAIN	4	1750,0	18817,2	0,0
MUGI	1309	5,3	280,9	1,8

Таблиця 9

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Core i7-5500u 2.4Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	657	10,7	0.08	6250,0
AES-256	1436	4,9	0.09	5555,6
HC-128	29	241,4	2982.80	0,2
HC-256	441	15,9	22889.10	0,0
MICKEY-128	9	777,8	4257.90	0,1
RABBIT	1215	5,8	80.80	6,2
SALSA-20	36	194,4	0.12	4166,7
SNOW2.0-128	50	140,0	91.70	5,5
SNOW2.0-256	100	70,0	90.30	5,5
SOSEMANUK	1550	4,5	101.60	4,9
STRUMOK 256	44	159,1	84.30	5,9
STRUMOK 512	44	159,1	105	4,8
TRIVIUM	66	106,1	219.90	2,3
CryptMT3	231	30,3	330,1	1,5
DECIM-128	2	3500,0	7889,9	0,1
RC4	6091	1,1	-	-
KCIPHER-2	182	38,5	751	0,7
GRAIN	5	1400,0	22713,3	0,0
MUGI	1609	4,4	326,7	1,5

Таблиця 10

Експериментальні результати дослідження шифрів за критерієм ініціалізація/генерація ключових параметрів (Intel Pentium P6200 2.13Gh)

Назва шифру	Встановлення ключових параметрів			
	Ключ (7000 установок)		Вектор ініціалізації (500 установок)	
	Час, μs	Швидкість, кількість установок / μs	Час, μs	Швидкість, кількість установок / μs
AES-128	944	7,4	0,1	5000,0
AES-256	2109	3,3	0,11	4545,5
HC-128	36	194,4	3648	0,1
HC-256	484	14,5	23303,2	0,0
MICKEY-128	13	538,5	5106,7	0,1
RABBIT	1804	3,9	115,6	4,3
SALSA-20	42	166,7	0,15	3333,3
SNOW2.0-128	58	120,7	107,8	4,6
SNOW2.0-256	114	61,4	109,4	4,6

SOSEMANUK	1878	3,7	121,9	4,1
STRUMOK 256	58	120,7	106,3	4,7
STRUMOK 512	58	120,7	104,7	4,8
TRIVIUM	78	89,7	256,3	2,0
CryptMT3	238	29,4	430,2	1,2
DECIM-128	2	3500,0	10634,2	0,0
RC4	10294	0,7	-	-
KCIPHER-2	235	29,8	1042,6	0,5
GRAIN	5	1400,0	27690	0,0
MUGI	2042	3,4	431,5	1,2

За отриманими показниками швидкості ініціалізації/генерації ключових параметрів можна зробити висновки, що найгірші значення у шифрів HC-128, HC-256, MICKEY-128. Це пояснює погані показники у HC-128 та HC-256 за критерієм шифрування коротких повідомлень – у алгоритмі багато часу витрачається на оновлення нових ключових параметрів. Найкращі показники мають AES-128, AES-256 та SALSA-20.

Висновки

Досліджені алгоритми ПСШ забезпечують високі криптографічні показники. Зокрема, виконуються вимоги статистичної безпеки, тобто послідовність, що сформована генераторами, не відрізняється за своїми статистичними властивостями від дійсно випадкової послідовності. Методики статистичних досліджень, які розглянуті в даній роботі, та отримані результати можуть розглядатися як первинний аналіз криптографічних властивостей генераторів, оскільки такі статистичні тести не враховують власну структуру генератора.

Наведені результати тестування різних потокових криптоперетворень підтверджують їхні високі криптографічні показники. Всі досліджувані шифри показали високе число успішно пройдених тестів: 130 – 134 за критерієм $P_j \geq 0{,}99$ та 186 – 187 за критерієм $P_j \geq 0{,}96$. Слід відмітити високі показники статистичної безпеки алгоритму ПСШ «Струмок», який виявив певні властивості генератору випадкових бітів. Зокрема, за своїми характеристиками сформовані послідовності не поступаються ПВП, які сформовано всесвітньо відомими потоковими криптографічними алгоритмами, зокрема шифрами HC-256 та SNOW 2.0. Крім того, для ПСШ «Струмок» мінімальні значення числа пройдених статистичних тестів за критерієм $P_j \geq 0{,}96$ є вищі, ніж у цих алгоритмах, що свідчить про незначну перевагу показників статистичної безпеки алгоритму «Струмок».

Результати статистичного тестування пакетом DIEHARD для симетричних шифрів AES, Enocoro, Grain, HC, MICKEY, MUGI, Salsa20, Sosemanuk, Trivium та ПСШ «Струмок» показують, що за більшістю показників всі потокові криптоалгоритмів мають порівняні показники статистичної безпеки. Для ПСШ «Струмок» додатково були проведені тести DIEHARD щодо розподілу ймовірностей, за результатами яких встановлено, що розподіл ймовірності відповідає рівномірному закону з невеликими флуктуаціями. Це додатково свідчить на користь висновку щодо високих показників статистичної безпеки цього алгоритму.

Результати тестування швидкодії показали, що за критерієм шифрування довгих повідомлень найкращі показники отримали «Струмок», HC-128 та SNOW 2.0. Причому, алгоритм «Струмок» дає кращі результати, ніж HC-128 на 30 %, та кращі за SNOW 2.0 майже удвічі. Експериментальні результати за критерієм шифрування коротких повідомлень

продемонстрували, що найкращі показники дає шифр «Струмок», SNOW 2.0 та SOSEMANUK відповідно. Шифри SNOW 2.0 та SOSEMANUK мають кращі показники в тому випадку, коли пакетів багато але малих за розміром. У потоковому шифрі «Струмок» результати зворотні: шифр демонструє кращі показники, коли пакети великі за розміром. За показниками критерію ініціалізація/генерація ключових параметрів найгірші показники у шифрів HC-128, HC-256, MICKEY-128. Це пояснює погані показники у HC-128 та HC-256 за критерієм шифрування коротких повідомлень – у алгоритмі багато часу витрачається на оновлення нових ключових параметрів. Найкращі ж показники мають AES-128, AES-256 та SALSA-20.

Таким чином, за результатами досліджень швидкодії встановлено, що в порівнянні з кращими світовими аналогами (потоковими криптоалгоритмами Grain, HC-128, HC-256, MICKEY, Rabbit, Salsa20, SNOW 2.0, Sosemanuk, Trivium) криптоалгоритм «Струмок» забезпечує найвищі (після HC-128 та HC-256) показники швидкості. Отже, алгоритм «Струмок» здатний забезпечувати високі показники швидкодії та ефективно функціонувати на різних обчислювальних платформах. Зазначимо, що ці оцінки не є граничними, тобто перспективним напрямком подальшої розробки є оптимізація програмної реалізації для збільшення пропускної здатності, наприклад за рахунок розпаралелювання або прискорення за рахунок залучення додаткових апаратних засобів.

Результати експериментальних досліджень статистичної безпеки та швидкісних характеристик потокових шифрів свідчать, що алгоритм «Струмок» є найбільш виваженим рішенням, він спроможний забезпечувати властивості генератора випадкових послідовностей та видавати величезні показники за швидкістю шифрування. Практично доведено, що швидкість шифрування алгоритмом «Струмок» на сучасних обчислювальних системах може досягати 10 – 15 Гбіт/с.

Список літератури: 1. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. – Харків : ХНУРЕ; Форт, 2012. – 868 с. 2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія : підручник. – Харків : ХНУРЕ; Форт, 2012. – 878 с. 3. *Есин В.І., Кузнецов О.О., Сорока Л.С.* Безпека інформаційних систем і технологій. – Харків : ХНУ ім. В.Н. Каразіна, 2013. – 632 с. 4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М. : Триумф, 2002. – 797 с. 5. *Розробка* нового блокового симетричного шифру: звіт за перший етап НДР «Алгоритм» (проміжний) / АТ «ІІТ» ; кер. І.Д. Горбенко – Харків, 2014. – Т. 4. – 304 с. 6. *ISO/IEC* 18033-4. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54532. 7. *ISO/IEC* 29192-3. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56426 8.*The eSTREAM* Project. [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org 9. *Cryptography* Research and Evaluation Committees. [Електронний ресурс]. – Режим доступу: http://www.cryptrec.go.jp/english/about.html 10. *Kuznetsov O. O., Ivanenko D.V., Lutsenko M.S.* Strumok stream cipher: spesification and basic properties // 2016 Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016). October 4 – 6, 2016 Ukraine, Kharkiv. – Kharkiv : IEEE, 2016. C. 59-62. 11. *Дослідження* потокових симетричних шифрів та потокових режимів блокових симетричних шифрів: звіт про НДР (заключний), шифр «Струмок». Т. 2. – Розробка пропозицій до проекту алгоритму потокового симетричного шифрування та обґрунтування його властивостей / ХНУ ім. В.Н. Каразіна ; кер. Кузнецов О.О. ; вик.: Малахов С.В. [та інш., всього 13 осіб]. – Харків : ХНУ ім. В.Н. Каразіна. – 2015. – 73 с. 12. *Thank* you Bob Anderson. Список рассылки Cypherpunks (9 сентября 1994). [Електронний ресурс]. – Режим доступу: http://cypherpunks.venona.com/date/1994/09/msg00304.html 13. *Bruce Schneier*. Applied cryptography. Second edition. John Wiley & Sons. 1996 14. *Andreas Klein*. Attacks on the RC4 stream cipher. [Електронний ресурс]. – Режим доступу: http://www.networklife.net/images/wep-rc4/RC4.pdf. 15.*FIPS-197*: Advanced Encryption Standard (AES). National Institute of Standards and Technology. – 2001. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. 16. *ISO/IEC* 18033-3. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:18033:-3:ed-2:v1:en 17. *NIST* Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf 18. *Потий А.В, Орлова С.Ю, Гриненко Т.А*. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та

метрологічне забезпечення захисту інформації в Україні. Вип.2, 2001. – С. 206 – 213. 19. *Кузнецов А.А., Мордвинов Р.И., Колованова Е.П., Самойлова А.В.* Методика статистического тестирования криптографических алгоритмов // Спеціальні телекомунікаційні системи та захист інформації. – Київ – 2014. – №1(25). – С.54-61. 20. *Diehard*er: A Random Number Test Suite. [Електронний ресурс]. – Режим доступу: http://www.phy.duke.edu/~rgb/General/dieharder.php 21.*The Marsaglia* Random Number CDROM including the Diehard Battery of Tests of Randomness. [Електронний ресурс]. – Режим доступу: http://stat.fsu.edu/pub/diehard/ 22. *Gjorgjievski, Sashe* (et al.). Relation Between Statistical Tests for Pseudo-Random Number Generators and Diaphony as a Measure of Uniform Distribution of Sequences. In: Stojanov, Georgi, Kulakov, Andrea (Eds.), ICT Innovations 2016. Cognitive Functions and Next Generation ICT Systems. Springer International Publishing, pp. 80-92. 23. *VeraCrypt*. [Електронний ресурс]. – Режим доступу: https://veracrypt.codeplex.com/ 24. *TrueCrypt*. [Електронний ресурс]. – Режим доступу: http://truecrypt.sourceforge.net/

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 15.09.2017

СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06:519.248.681

И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук

АНАЛИТИЧЕСКАЯ ОЦЕНКА ЗНАЧЕНИЙ МАКСИМАЛЬНЫХ БОКОВЫХ ЛЕПЕСТКОВ ФУНКЦИЙ КОРРЕЛЯЦИИ СЛОЖНЫХ НЕЛИНЕЙНЫХ ДИСКРЕТНЫХ СИГНАЛОВ

Введение

Используемые в информационно-коммуникационных системах (ИКС) в качестве физических переносчиков данных множества линейных дискретных сигналов не позволяют в ряде случаев обеспечить необходимые показатели информационной безопасности и помехозащищенности [1 – 5]. Они могут быть улучшены посредством применения систем нелинейных дискретных сигналов. Однако для этого необходимо оценивать граничные значения корреляционных функций, например минимаксные свойства и соответствие границе «плотной упаковки».

В [3] указаны принципиально достижимые значения максимальных боковых пиков периодической функции автокорреляции (ПФАК), т.е. соответствие границы «плотной упаковки» в зависимости от заданного периода последовательности N:

$$R_{max}^{a} \geq \begin{cases} 0, \text{ если } N \equiv 0 (\text{mod } 4); \\ 1, \text{ если } N \equiv 1 (\text{mod } 4); \\ 2, \text{ если } N \equiv 2 (\text{mod } 4); \\ -1, \text{ если } N \equiv 3 (\text{mod } 4), \end{cases} \quad (1)$$

Приведенные границы устанавливают критерий синтеза множества ДП (сигнатур). Ансамбли, со значениями R_{max}, достигающие предела, предсказываемого границами (1), являются оптимальными по критерию корреляционного пика и называются минимаксными.

Цель настоящей статьи – получение аналитических соотношений минимаксных оценок корреляционных свойств широкого класса нелинейных дискретных сигналов с учетом ограничений (1).

Постановка задачи исследований

К числу привлекательных для рассмотрения, с точки зрения корреляционных и ансамблевых свойств, отнесем нелинейные характеристические дискретные сигналы (ХДС) с числом позиций $N = 4x + 2$ и $N = 4x, x = 1, 2, \ldots$[5]. Построение данных ХДС базируется на использовании характера мультипликативной группы $\Psi(x)$ поля $GF\left(P^n\right), n \geq 1$.

Правило построения таких ДП для $L = 4x + 2$ имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P - 2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (2)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (3)$$

где Θ – первообразный элемент поля $GF(P)$.

Для $L = 4x$ правило кодирования имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P - 2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P), \quad (4)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0(\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P). \quad (5)$$

В [5] показано, что мощность метода данного класса сигналов (M) равна числу классов не инверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \phi(L)/2\cdot$, где (φ(L)) – функция Эйлера. Известно также [5], что правила (2) – (5) приводят к ДП с двухуровневой периодической функцией автокорреляции (ПФАК) и значения боковых пиков ПФАК для правил (2) – (3) составляет $R_\mu = \{-2, 2\}$, а для правил кодирования (4) и (5) значения боковых пиков ПФАК составляет $R_\mu = \{0, -4\}$ и $R_\mu = \{0, 4\}$ соответственно.

В соответствии с (1) системы таких нелинейных ХДС являются плотноупакованными по периодической функции корреляции (ПФАК), существуют для большого спектра длительностей N, однако размерность ансамбля ХДС ограничена значением функции Эйлера от периода сигнала. Проведенные исследования показали [6 – 10], что дальнейшее увеличение размерности ансамбля и улучшение структурных свойств сигналов, составляющих ансамбль, может быть достигнуто на основе использования L-позиционных (производных) нелинейных сигналов, построение которых осуществляется посредством образования последовательного произведения $Z_i, i = \overline{1,k}$, символов W_j^i нелинейных сигналов с одно- или двухуровневой ПФАК.

Аналитические оценки корреляционных свойств производных нелинейных сигналов

Правило построения символов W_i^p производных нелинейных сигналов (ПНС) сформулируем в виде

$$W_i^p = \prod_{j=1}^{k} W_{i(\text{mod}\, L_i),j} \quad (6)$$

Значения боковых пиков ПФАК, для ПНС, построенных по (1), найдем, используя соотношение $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i+l}^j\right)^*$:

$$R_w^p(l) = \sum_{i=0}^{L-1} \prod_{j=r}^{K_1} W_{i(\text{mod}\, L_i),j} \prod_{j=1}^{K_2} W_{i+l(\text{mod}\, L_i),j}, \quad (7)$$

где $K_1 \neq K_2$.

Анализ корреляционных свойств с использованием (45) в общем виде затруднен, поэтому рассмотрим ряд частных случаев, важных как с теоретической, так и с практической точек зрения.

1. Пусть $K_1 = K_2$, а $L_1 \neq L_2$, тогда (7) имеет вид

$$R_w(l) = \sum_{i=0}^{L-1} W_{i(\text{mod}\, L_1),i} \cdot W_{i+l(\text{mod}\, L_1),1} \cdot W_{i(\text{mod}\, L_1),2} \cdot W_{i+l(\text{mod}\, L_2),2}. \quad (8)$$

Для преобразования (8) представим индекс суммирования i в L_2-ричной системе счисления как

$$i = \upsilon L_2 + \varepsilon, \quad 0 \le \varepsilon \le L_2, \; 0 \le \upsilon \le L_1 \tag{9}$$

$$R_w(l) = \sum_{\upsilon=0}^{L_1-1}\sum_{\varepsilon=0}^{L_2-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_1),1}\cdot W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_2),2}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L_1),2}\cdot W_{\upsilon L_2+\varepsilon l(\mathrm{mod}\,L_2),2} = \sum_{\varepsilon=0}^{L_1-1} W_{\varepsilon(\mathrm{mod}\,L_1),1}\cdot \tag{10}$$

$$\times W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L1),1}.$$

С учетом, того, что $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i+l}^j\right)^*$,

$$\sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\mathrm{mod}\,L_2),2}\cdot W_{\varepsilon+l(\mathrm{mod}\,L_2),2} = R_{W_2}(l) \tag{11}$$

Кроме того, если υ принимает значение из множества вычетов по $\mathrm{mod}\,L_1$, то $\upsilon L_2 + \varepsilon$ пробегает значения по модулю L_1, поэтому

$$\sum_{\varepsilon=0}^{L_1-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_1),1}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L_1),1} = \sum_{q=0}^{L_1-1} W_{q(\mathrm{mod}\,L_1),1}\cdot W_{q+\varepsilon(\mathrm{mod}\,L_1),1} = R_{W_1}(l) \tag{12}$$

и ПФАК ПНС может быть рассчитана с использованием выражения

$$R_{W^n}(l) = R_{W_1}(l)\cdot R_{W_2}(l). \tag{13}$$

Но, так как $R_{W_1}(l)$ и $R_{W_2}(l)$ могут принимать соответственно значения L_1 и L_2 при $l = 0$, $R_{W_1}(l)$ и $R_{W_2}(l)$ при $l = \overline{1, L-1}$, то

$$R_{W^n}(l) = \begin{cases} L, & \text{при } l \equiv 0(\mathrm{mod}\,L); \\ L_2 R_{W_1}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_2),\ L \ne 0\ (\mathrm{mod}\,L_1); \\ L_1 R_{W_2}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1),\ l \ne 0(\mathrm{mod}\,L_2); \\ R_{W_1}(l)\cdot R_{W_2}(l), & \text{при } l \ne 0(\mathrm{mod}\,L_1, \mathrm{mod}\,L_2). \end{cases} \tag{14}$$

Анализ (14) показывает, что минимальные боковые лепестки ПНС имеют место в случае, если L_2, $R_{w_1}(l)$, L_1, $R_{w_2}(l)$ принимают минимальные значения.

2. Пусть $K = 3$, а $L_1 \ne L_2 \ne L_3$. В этом случае по аналогии с (14) выражение (7) можно представить в виде

$$R_{W^n}(l) = R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \tag{15}$$

или

$$R_{W^n}(l) = \begin{cases} L, & \text{при } l \equiv 0(\mathrm{mod}\,L); \\ R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), & \text{при } l \ne 0(\mathrm{mod}\,L_1, L_2, L_3); \\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1),\ l \ne 0(\mathrm{mod}\,L_2, L_3); \\ L_2\cdot R_{W_1}(l)\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_2),\ l \ne 0(\mathrm{mod}\,L_1, L_3); \\ L_3\cdot R_{W_1}(l)\cdot R_{W_2}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_3),\ l \ne 0(\mathrm{mod}\,L_1, L_2); \\ L_1\cdot R_{W_2}(l)\cdot L_3, & \text{при } l \equiv 0(\mathrm{mod}\,L_1, L_3),\ l \ne 0(\mathrm{mod}\,L_2); \\ L_1\cdot L_2\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1, L_2),\ l \ne 0(\mathrm{mod}\,L_3); \\ R_{W_1}(l)\cdot L_2\cdot L_3, & \text{при } l \equiv 0(\mathrm{mod}\,L_2, L_3),\ l \ne 0(\mathrm{mod}\,L_1). \end{cases} \tag{16}$$

Анализ (16) показывает, что для минимизации $R_{W^n}(l)$ необходимо и достаточно, чтобы $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W3}(l)$ были минимальными, а L_1, L_2 и L_3 – минимальными и взаимно простыми. Минимальное значение R_{W_i}, $i=\overline{1,3}$, равное 0, достигается только при использовании в качестве W_1 последовательности [3] вида {1 1 1 -1}. В этом случае выражение (16) принимает вид

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L); & \text{а)}\\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3); & \text{б)}\\ L_1\cdot R_{W_3}(l)\cdot L_2, \quad \text{при } l\equiv 0(\text{mod } L_1, L_2),\ l\neq 0(\text{mod } L_3); & \text{в)}\\ L_1\cdot R_{W_2}(l)\cdot L_3, \quad \text{при } l\equiv 0(\text{mod } L_1, L_3),\ l\neq 0(\text{mod } L_2). & \text{г)} \end{cases} \qquad (17)$$

Исследование выражений (17) (а, б и г), показывает, что для их минимизации необходимо, чтобы как принимаемые значения ПФАК $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W_3}(l)$, так и значения их длительностей были минимальными. С учетом того, что $L_1=4$, максимальные значения ПФАК $R_W(l)$ дают слагаемые в) и г) (выражение (17). Если L_2 и L_3 – взаимно простые, то минимальные значения $R_{W_2}(l)$ и $R_{W_3}(l)$ могут быть соответственно равны $\{\pm 1\}$ и $\{-4, 0\}$ или $\{0, 4\}$, или $\{2, -2\}$, поэтому

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L); & \text{а)}\\ \pm 4, \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3); & \text{б)}\\ \pm 4L_1L_2, \quad \text{при } l\equiv 0(\text{mod } L_1, L_2),\ l\neq 0(\text{mod } L_3); & \text{в)}\\ \pm L_1L_3, \quad \text{при } l\equiv 0(\text{mod } L_1, L_3),\ l\neq 0(\text{mod } L_2). & \text{г)} \end{cases} \qquad (18)$$

Если L_1 и L_2 – взаимнопростые, то выражение $\pm 4L_1L_2$ принимает значение либо $\pm 4L_1R_{W_2}(l)$, либо $\pm 4R_{W_1}(l)L_2$, поэтому максимальный боковой лепесток дает составляющая $\pm L_1L_3$.

Из приведенного следует, что для минимизации боковых лепестков необходимо, чтобы L_1, L_2 и L_3 были взаимнопростыми. Этого можно достичь, если L_1 и L_2 – простые, а $L_3\equiv 0(\text{mod } 2)$. При этих условиях составляющие (11) принимают значения

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L);\\ R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\neq 0(\text{mod } L_1, L_2, L_3);\\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3);\\ L_2\cdot R_{W_1}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_2),\ l\neq 0(\text{mod } L_1, L_3);\\ L_3\cdot R_{W_1}(l)\cdot R_{W_2}(l), \quad \text{при } l\equiv 0(\text{mod } L_3),\ l\neq 0(\text{mod } L_1, L_3). \end{cases} \qquad (19)$$

3. Пусть $L_1=L_2=L_K=L$, а $K_1=K_2=K$. Для этих условий с учетом (2) выражение для ПФАК ПНС можно представить в виде

$$R_{W_n}(l)=\sum_{i=0}^{L-1}\prod_{j=1}^{K}W_{i,j}^{q}\prod_{j=1}^{K}W_{i+l,j}, \qquad (20)$$

причем (20) позволяет вычислить ПФАК, если положить, что $q=r$.

Проведенные исследования показали, что для рсчетов (20) можно получить оценки, если воспользоваться теорией двухзначных характеров, в частности, тем, что для любого нетривиального характера справедливо [5]

$$\sum_{y \in GF(P)} \Psi(ay+b) = \sum_{\substack{y \in GF(P^W) \\ y \neq 0 (\mathrm{mod}\, P)}} \Psi(ay+b) + \Psi(b) = 0,$$

и фиксированными правилами кодирования. Например, для наиболее мощного класса двухуровневых последовательностей – последовательностей характеристического типа с числом символов $L = 2x = P^n - 1$, $x = 1, 2, 3, \ldots, z, \ldots$

$$W^q = \left\{ W_i^q, \quad i = \overline{0, P^n - 1} \right\};$$

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0 [\mathrm{mod}\, f(x), P]; \\ 1, & \text{если } \Theta_q^i + 1 \equiv 0 [\mathrm{mod}\, f(x), P]; \end{cases} \quad \text{а)}$$

либо

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0 [\mathrm{mod}\, f_m(x), P]; \\ -1, & \text{если } \Theta_q^i + 1 \equiv 0 [\mathrm{mod}\, f_m(x), P]; \end{cases} \quad \text{б)} \qquad (21)$$

где Θ_q – q-й первообразный элемент поля $GF(P)$, а $f_m(x)$ – m-й первообразный примитивный полином степени n.

Приведем вывод аналитического выражения для ПФАК ПНС. Используя (19) и полагая, что $q \neq r$, имеем

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1). \qquad (22)$$

С учетом того, что $\Psi(0) = 0$, [ ], при $l \neq 0 (\mathrm{mod}\, L)$

$$R_{W_n}(l) = \sum_{i=0}^{P^n - 2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1) \pm Z, \qquad (23)$$

где Z – учитывает сумму слагаемых, входящих в (23), для которых

$$\left(\Theta_q^i + 1\right) \equiv 0 \vee \left(\Theta_q^{i+l} + 1\right) \equiv \left(\Theta_r^i + 1\right) \equiv \left(\Theta_r^{i+l} + 1\right) \equiv 0 [\mathrm{mod}\, f_m(x), P] \qquad (24)$$

Более точно структуру (62) определяют сформулированные ниже утверждения.

Утверждение 1. Пусть $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ есть элементы поля $GF(P^n)$ а Θ_υ^υ – υ-й первообразный элемент, тогда при $l' \neq 0 (\mathrm{mod}\, L)$ $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ никогда не сравнимы с $0 [\mathrm{mod}\, f_m(x), P]$. Доказательство утверждения следует из цикличности поля $GF(P^n)$ [4].

Утверждение 2. Пусть $\Theta_\upsilon^r + 1$ и $\Theta_k^m + 1$ – элементы поля $GF(P^n)$, а Θ_υ и Θ_k – первообразные. Существуют T^{s1} и T^{s2} автоморфные преобразования, при которых

$$\Theta_\upsilon^r + 1 \equiv \Theta_k^m + 1 \equiv 0 (\mathrm{mod}\, L).$$

Доказательство утверждения следует из авто- и изоморфных свойств поля $GF(P^n)$ [5].

Выражение (24) распадается на следующие логические высказывания.

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^{i+l} \neq 0 (\mathrm{mod}\, L); \quad \text{а)}$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \neq 0 (\mathrm{mod}\, L); \quad \text{б)}$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \equiv 0 (\mathrm{mod}\, L); \quad \text{в)} \qquad (25)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \neq 0 (\mathrm{mod}\, L); \quad \text{г)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\equiv 0\wedge\Theta_r^i+1\equiv 0\wedge\Theta_r^{i+l}+1\neq 0(\mathrm{mod}\,L);\qquad \text{д)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\equiv 0\wedge\Theta_r^i+1\neq 0\wedge\Theta_r^{i+l}+1\equiv 0(\mathrm{mod}\,L);\qquad \text{е)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\neq 0\wedge\Theta_r^i+1\equiv 0\wedge\Theta_r^{i+l}+1\neq 0(\mathrm{mod}\,L);\qquad \text{ж}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\neq 0\wedge\Theta_r^i+1\neq 0\wedge\Theta_r^{i+l}+1\equiv 0(\mathrm{mod}\,L).\qquad \text{з)}$$

Анализ (25) показывает, что исключающими являются высказывания а), г), ж), з), поэтому

$$\begin{gathered}Z=\Psi\left(-\Theta_q^{i+l}+1\right)\cdot\Psi\left(-\Theta_r^i+1\right)\cdot\Psi\left(-\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_q^{-l}+1\right)\cdot\Psi\left(\Theta_r^i+1\right),\\ \Psi=\left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_r^l+1\right)\cdot\Psi\left(\Theta_q^i+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+\\ +\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^i+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\end{gathered}. \tag{26}$$

Действительно, если истинно выражение (63), а), то $\Psi\left(\Theta_q^i+1\right)=0$, так как $\Theta_q^i+1\equiv 0(\mathrm{mod}\,L)$ [5], поэтому

$$\Psi\left(\Theta_q^{i+l}+1\right)=\Psi\left[\Theta_q^l\left(\Theta_q^i+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^l\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(\Theta_q^l\cdot\Theta_q^{-l}-\Theta_q^l\right)=\Psi\left(1-\Theta_q^l\right)=\Psi\left(-\Theta_q^l+1\right).$$

В случае, если $\Theta^{i+l}+1\equiv 0(\mathrm{mod}\,L)$, то

$$\Psi\left(\Theta_q^i+1\right)=-\Psi\left(\Theta_q^i\cdot\Theta_q^l\cdot\Theta_1^{-l}+1\right)=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{i+l}+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(-\Theta_q^{-l}+1\right).$$

Преобразуем выражение (23), используя свойство характера Ψ [5], обозначив его переменной X:

$$\begin{gathered}X=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^{i+l}+1\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^{i+l}+1\right)=\\ =\Psi\left(\Theta_q^i\right)\cdot\Psi\left(\Theta_r^i\right)\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^i+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^i+\Theta_r^{-l}\right)=\Psi\left(\Theta_q^l\right)\cdot\Psi\left(\Theta_r^l\right)\cdot Q\end{gathered} \tag{27}$$

Проанализируем выражение

$$Q=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^i+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^i+\Theta_r^{-l}\right).$$

Учитывая, что если i принимает значения индексов суммирования, то степени первообразных элементов Θ_q и Θ_r принимают значения всех ненулевых элементов поля $GF(P^n)$. Обозначая ненулевые элементы поля через a_i и b_i соответственно для первообразных Θ_q и Θ_r, при $i=\overline{0,P^n-2}$, перейдем к сумме произведения характеров ненулевых элементов

$$Q=\sum_{a_i,b_i\in GF(P^n)}\Psi\left(a_i+1\right)\cdot\Psi\left(a_i+\Theta_q^{-l}\right)\cdot\Psi\left(b_i+1\right)\cdot\Psi\left(b_i+\Theta_r^{-l}\right). \tag{28}$$

Полагая в (28) $c_i=a_i+1$ и $d_i=b_i+1$, проанализируем все c_i и d_i, если a_i и b_i пробегают все значения ненулевых элементов поля $GF(P^n)$, то c_i и d_i так же пробегают все ненулевые элементы поля $GF(P^n)$ исключая 1, поэтому

$$Q=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi\left(c_i\right)\cdot\Psi\left(c_i+\Theta_q^{-l}+1\right)\cdot\Psi\left(d_i\right)\cdot\Psi\left(d_i+\Theta_r^{-l}-1\right). \tag{29}$$

Если же

$$\begin{aligned} &c_i = 1, \quad \text{то } Q_1 = \Psi\left(\Theta_1^{-l}\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l} - 1\right); && \text{а)} \\ &d_i = 1, \quad \text{то } Q_2 = \Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right); && \text{б)} \\ &c_i = 1, d_i = 1, \quad \text{то } Q_3 = \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right); && \text{в)} \end{aligned} \tag{30}$$

Исключим в (28) условие $c_i, d_i \neq 1 (\mathrm{mod}\, P)$, для этого добавим в него и вычтем Q_1, Q_2 и Q_3. В результате получим

$$\begin{aligned} Q = &\sum \Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l}\right) - \Psi\left(\Theta_q^{-l}\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l} - 1\right) - \\ &-\Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right) - \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right) = \\ = &\sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(c_i^{\,2}\right)\Psi\left(1 + \left(\Theta_q^{-l} - 1\right)c_i^{-1}\right)\Psi\left(d_i^{\,2}\right)\Psi\left[1 + \left(\Theta_r^{-l} - 1\right)d_i^{-1}\right] - Q_1 - Q_2 - Q_3. \end{aligned} \tag{31}$$

Принимая во внимание, что $\Theta_q^{-l} - 1$ и $\Theta_r^{-l} - 1 \in GF(P^n)$ являются постоянными, обозначив их как $q_1 = \Theta_q^{-p} - 1$ и $q_2 = \Theta_r^{-l} - 1$, $q_1, q_2 \neq 0 (\mathrm{mod}\, P)$, а также обозначив $x_i = c_i^{-1}$ и $y_i = d_i^{-1}$, которые пробегают так же все элементы поля $GF(P^n)$, получим

$$Q = \sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(1 + q_i x_i\right)\Psi\left(1 + q_2 y_2\right) - Q_1 - Q_2 - Q_3.$$

С учетом (26), (28), (30), выражение (23) может быть представлено как:

$$\begin{aligned} R_{W^n}(l) = &\Psi\left(\Theta_q^{l}\right)\Psi\left(\Theta_r^{l}\right)\{\sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(1 + q_i x_i\right)\Psi\left(1 + q_2 y_1\right) - [\Psi\left(\Theta_q^{-l}\right) \cdot \Psi\left(d_i\right)\Psi\left(d_i - \Theta_r^{-l} - 1\right) + \\ &+\Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right) + \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right)]\} + \{\Psi\left(-\Theta_q^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_q^{-l} + 1\right)\Psi\left(\Theta_r^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_r^{-l} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\}, \end{aligned} \tag{32}$$

где запись $\{y\}$ означает, что слагаемые в скобках необходимо брать со знаками $+(-)$ во всевозможных сочетаниях, то есть 2^k сочетаний, если k – число слагаемых.

Упростим (32) учитывая, что все слагаемые

$$\begin{aligned} &\Psi\left(\Theta_q^{l}\right), \Psi\left(\Theta_r^{l}\right)\Psi\left(\Theta_q^{-l}\right), \Psi\left(d_i\right), \Psi\left(d_i - \Theta_r^{-l} - 1\right), \ldots, \\ &\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) \in \{1; -1\}. \end{aligned} \tag{33}$$

Из (32) непосредственно следует, что

$$\begin{aligned} Z = \pm\{&\Psi\left(-\Theta_q^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_q^{-l} + 1\right)\Psi\left(\Theta_r^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\} \end{aligned}$$

принимает значение на множестве чисел $Z' = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. Поэтому, используя (33), выражение (32) можно представить в виде

$$R_{W^n}(l)=\{\pm\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}\,P)}}\Psi\left(1+q_1x_i\right)\Psi\left(1+q_2y_i\right)\pm[3]\}\pm[4], \tag{34}$$

где запись [3] и [4] означает, что вместо [3] при анализе необходимо использовать числа $(-3,-2,-1,0,1,2,3)$, а вместо [4] – числа $(-4,-3,-2,-1,0,1,2,3,4)$.

Рассмотрим вывод аналитического выражения для ПФВК ПНС. Используя выражение для расчета функции взаимной корреляции

$$R^{\upsilon}_{j,m}(l)=\sum_{i=1}^{L-k}W_i^{\upsilon}\left(W_{i+1}^{j}\right)^*+\sum_{i=L-k+1}^{L}W_i^{\upsilon}\left(W_{i-L+k}^{m}\right)^*,$$

получим $(j=m)$

$$R^{B}_{W^n}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right). \tag{35}$$

Приведем вывод выражения для оценки выбросов ПФВК

$$R^{B}_{W^n}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i-l}_{r_4}+1\right). \tag{36}$$

Далее, аналогично выражению (36)

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\cdot\Psi(\Theta^i_{r_2}+1)\cdot\Psi(\Theta^{i+l}_{r_3}-1)\cdot\Psi\left(\Theta^{i+l}_{r_4}-1\right)\pm Z, \tag{37}$$

где Z представляет собой сумму слагаемых, входящих в (36), для которых $\Theta^i_{r_1}+1\equiv 0\vee\left(\Theta^i_{r_2}+1\right)\equiv 0\vee\left(\Theta^{i+l}_{r_3}+1\right)\equiv 0\vee\left(\Theta^{i+l}_{r_4}+1\right)\equiv 0$, что эквивалентно:

$$\Theta^i_{r_1}+1\equiv 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{а)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\equiv 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{б)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\equiv 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{в)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\equiv 0(\mathrm{mod}\,L); \quad \text{г)}$$

поэтому:

$$\begin{aligned}Z=\pm\{&\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i+l}_{r4}+1\right)+\\&+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta_{r_3i+l}+1\right)+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)\},\end{aligned} \tag{38}$$

может принимать значения на множестве $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$, следовательно (37) есть

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\cdot\Psi(\Theta^i_{r_2}+1)\cdot\Psi(\Theta^{i+l}_{r_3}+1)\cdot\Psi\left(\Theta^{i+l}_{r_4}+1\right)\pm[4]=x\pm[4]. \tag{39}$$

Преобразуем выражение для x следующим образом:

$$\begin{aligned}x=&\Psi\left(\Theta^l_{r_3}\right)\Psi\left(\Theta^l_{r_4}\right)\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\Psi(\Theta^i_{r_2}+1)\Psi(\Theta^i_{r_3}+\Theta^{-l}_{r_3})\Psi(\Theta^i_{r_4}+\Theta^{-l}_{r_4})=\\&=\Psi(\Theta^l_{r_3})\Psi(\Theta^l_{r_4})\cdot Q.\end{aligned} \tag{40}$$

Далее, выражение для Q (обозначив $\Theta^i_{r_1}+1=a_i$ и $\Theta^i_{r_2}+1=b_i$), представим в виде

$$Q=\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i,b_i\neq 1(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi\left(\Theta^i_{r_3}+\Theta^{-1}_{r_3}\right)\Psi\left(\Theta^i_{r_4}+\Theta^{-1}_{r_4}\right).$$

С учетом (29), (30), а также учитывая, что $\Theta^{-1}_{r_3}$ и $\Theta^{-1}_{r_4}$ могут принимать все значения из $GF(P^n)$, обозначив $c_i=\Theta^i_{r_s}+\Theta^{-1}_{r_s}$ и $d_i=\Theta^4_{r_4}+\Theta^{-1}_{r_4}$, причем, так как, во-первых, $\Theta^i_{r_3}\neq 0(\mathrm{mod}\,P)$ и $\Theta^{-1}_{r_3}\neq 1(\mathrm{mod}\,P)$, $\Theta^i_{r_3}+\Theta^{-1}_{r_3}\neq 1(\mathrm{mod}\,P)$, а во-вторых, при $\Theta^i_{r_4}\neq 0(\mathrm{mod}\,P)$ и $\Theta^{-1}_{r_4}\neq 1(\mathrm{mod}\,P)$, $\Theta^i_{r_4}+\Theta^{-1}_{r_4}\neq 1(\mathrm{mod}\,P)$, (40) можно представить в виде

$$\begin{aligned}R^B_{W^n}(l)&=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[4]\pm[15]=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[19].\end{aligned}\qquad(41)$$

Анализ (41) показывает, что элементы полей c_i,d_i представляют собой автоморфизмы полей $\Theta^i_{r_3}$ и $\Theta^i_{r_4}$ при $i=\overline{0,P^{n-2}}$. Сумма в нем берется по всевозможным произведениям характеров над $a_i,b_i,c_i,d_i\in GF(P^n)$ и дает оценку для максимально достигаемого выброса $R^B_{W^n}(l)_{max}$. С учетом того, что элементы a_i, b_i, c_i и d_i строятся по различным первообразным и пары условий

$$\Psi(a_i)=\Psi(1)\wedge\Psi(b_i)=\Psi(1);$$
$$\Psi(c_i)=\Psi(1)\wedge\Psi(d_i)=\Psi(1)$$

не истинны, и (41) имеет вид

$$\begin{aligned}R_{W^n}(l)&=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[8]\pm[4]=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[4]\pm[12].\end{aligned}\qquad(42)$$

Важной задачей является несбалансированность ПНС по числу символов $(+1)$ и (-1). Если $\Theta_1,\Theta_2,\ldots,\Theta_k$ – первообразные элементы поля $GF(P^n)$, то несбалансированность в числе символов есть

$$R_{W^n}(0)=\sum_{i=0}^{L-1}\prod_{j=1}^{k}\Psi\left(\Theta^i_j+1\right).$$

При $k=2$ аналогично (37)

$$R_{W^n}(0)=\sum_{i=0}^{P^n-2}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)=\sum_{i=0}^{P^n-2}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\pm Z,$$

где Z представляет собой сумму слагаемых, для которых

$$\Theta^{i}_{r_1}+1=0\vee\Theta^{i}_{r_2}+1\equiv 0(\mathrm{mod}\,P), \tag{43}$$

то есть

$$Z=\pm\Psi\left(\Theta^{i}_{r_1}+1\right)+\Psi\left(\Theta^{i}_{r_2}+1\right)\to\pm 2 \tag{44}$$

Далее обозначив $a_i=\Theta^{i}_{r_1}$ и $b_i=\Theta^{i}_{r_2}$, а затем $c_i=a_i+1$ и $d_i=b_i+1$ аналогично (26) – (30), имеем

$$\begin{aligned} x=&\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i,b_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i+1)\Psi(b_i+1)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)=\\ &\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)-\Psi(c_i)-\Psi(d_i)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[2]\end{aligned} \tag{45}$$

С учетом (45)

$$R^{B}_{W^n}(0)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[4]. \tag{46}$$

Заметим, что для случая $k=4$, $R_{W^n}(0)$ можно оценить, используя соотношения (42), то есть

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[12]. \tag{47}$$

Анализ (47) показывает, что несбалансированность, а следовательно, и шумы неортогональности с увеличением k увеличиваются и уже при $k=4$ достигают значительной величины, даже без учета результатов сумм в (46) и (47).

Особенности вычисления выражений (34), (42) и оценки их значений рассмотрим с использованием выражения (47). Воспользовавшись свойством функции характеров, имеем

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i,b_i,c_i,d_i)\pm 12. \tag{48}$$

Для случая двухзначного характера

$$R^{B}_{W^n}(0)=\sum_{u^{*}_i\in GF(P^n)}\exp\left(-j\pi u^{*}_i\right)\pm 12. \tag{49}$$

Исследование мощности изоморфного кодирования (объема системы сигналов или ансамбль сигналов), предпочтительно выполнять на основе изучения изоморфизмов разностных множеств. В [5] показано, что каждому коэффициенту разностных множеств может быть поставлен в соответствие первообразный элемент поля $GF(p^n)$.

В табл. 1 приведены значения объема системы сигналов M для некоторых значений периода последовательности L характеристических дискретных сигналов (ХДС).

Таблица 1

L_i	40	70	100	256	508	520	1020	1030	2052	2068	2080	2082	2098
M	8	12	20	64	126	96	125	204	515	460	384	346	524

Важной составляющей ансамблевых свойств системы сигналов является спектр значений периода сигналов, для которых могут быть синтезированы сигналы данной системы. В табл. 2 приведены значения числа ХДС, которые могут быть синтезированы в некотором интервале ς периодов сигналов.

Таблица 2

ς	2-100	100-200	200-300	300-400	400-500	500-600	600-700	700-800	800-900	900-1000	1000-1200
K	30	20	16	16	17	14	15	14	15	14	28

В табл. 3 приведены обобщенные данные о числе значений длин сигналов и объеме системы сигналов для m-последовательностей и ХДС.

Таблица 3

	Число значений L		Объем системы	
ΔL	ХДС	m-последовательностей	ХДС	m-последовательностей
$0-10^2$	30	4	456	8
$0-10^3$	186	9	29291	79
$0-10^4$	1269	11	2152943	554

Анализ приведенных в табл. 1 – 3 данных свидетельствует о том, что ХДС, с точки зрения ансамблевых свойств, являются более предпочтительными по сравнению с целым рядом широко используемых в различных приложениях ИКС линейных классов сигналов (m-последовательности, последовательности Лежандра и другие). Например, на интервале длин от 50 до 1500 m-последовательности существуют только для пяти значений периода, доступное число последовательностей Лежандра составляет 114, число характеристических сигналов для этого интервала длин составляет 225. Более того, мощность метода кодирования для ХДС определяется числом классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $\mathbf{T} = \{t\}\ \{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов и равна $\Psi(N)/2n$. Так для ХДС с числом элементов $N = 2052$ существует 515 изоморфизмов данного кода, в то время как для m-последовательностей ($N = 2047$) только 88 изоморфизмов. Объем системы, составленной из ХДС в интервале длительностей до 10000 символов, более чем в 10^3 раз превышает объем системы, составленной из m-последовательностей. Система сигналов может быть расширена за счет привлечения автоморфизмов (циклических сдвигов) изоморфных сигналов. Указанное становится возможным в том случае, если все множество циклических сдвигов (или отдельные автоморфизмы) обладают необходимыми корреляционными свойствами. Мощность авто- и изоморфного кодирования $M_{аи}$ в классе характеристических дискретных сигналов при заданном периоде последовательности N может быть определена из соотношения

$$M_{аи} = N\varphi(N)/2n. \qquad (50)$$

В классе производных характеристических сигналов, построенных по правилу (2) при k = 2, мощность производного авто- и изоморфного кодирования

$$M_{паи} = (N+2)\varphi(N)(\varphi(N) - 2n)/\ 8n^2\ . \qquad (51)$$

В табл. 4 приведены значения $M_{паи}$ для некоторых значений L, вычисленных с использованием соотношения (51).

Таблица 4

L	66	100	130	256	508	1018	2098
$M_{паи}$	$3{,}1\ 10^3$	$1{,}9\cdot10^4$	$3{,}7\cdot10^4$	$5{,}2\cdot10^5$	$4{,}0\cdot10^6$	$3{,}3\cdot10^7$	$2{,}9\cdot10^8$
L	3000	4000	5002	6010	7012	8008	9010
$M_{паи}$	$2{,}4\cdot10^8$	$1{,}3\cdot10^8$	$3{,}6\cdot10^9$	$4{,}3\cdot10^9$	$1{,}1\cdot10^{10}$	$8{,}3\cdot10^9$	$1{,}2\cdot10^{10}$

Таким образом, аналитические соотношения (14), (19) а также и (41) – (48) позволяют получить минимаксные оценки корреляционных свойств класса производных характеристи-

ческих дискретных сигналов. Такой подход применим и для оценки корреляционных свойств и других классов дискретных плотно упакованных по ПФАК дискретных сигналов.

Выводы

Анализ выражения (49) показывает, что оценка максимальных боковых лепестков ПФАК, ПФВК и несбалансированности в числе символов (1) и (-1) может быть сведена к изучению несбалансированности по четности и нечетности индексов производного поля, элементами которого являются числа (полиномы) вида $x_i = a_i \cdot b_i \cdot c_i \cdot d_i\left[\mathrm{mod}\, f(x), P\right]$. Анализ выражения (48) показывает, что для анализа нелинейных сигналов (ПНС) по критерию минимума максимальных выбросов $R^{B}_{W}(l)\left(R^{B}_{W^n}(l)\right)$, с точки зрения вычислительной сложности, предпочтительнее использовать алгоритм (48), а при вычислении основных статистических характеристик – алгоритм (49). Характеристические дискретные сигналы, с точки зрения корреляционных свойства автокорреляционной функции, отвечают границе «плотной упаковки» (1). Указанное позволяет обеспечить высокие показатели помехоустойчивости приема сигналов в условиях воздействия структурных, имитационных, ретранслированных и некоторых других типов помех.

Использование в современных ИКС производных нелинейных характеристических дискретных сигналов позволит существенно улучшить ансамблевые свойства физических переносчиков данных, что, в свою очередь, повысит уровень крипто- и имитозащищенности информационного обмена.

Список литературы: 1. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків : Форт, 2012. – 880 с. 2. *Горбенко, Ю.І.* Методи побудування та аналізу, стандартизація та застосування криптографічних систем / Ю.І. Горбенко. – Харків : Форт, 2016. – 959 с. 3. *Варакин, Л. Е.* Системы связи с шумоподобными сигналами / Л. Е Варакин. – М. : Радио и связь, 1985. – 384 с. 4. *Замула, А.А.* Перспективы применения нелинейных дискретних сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. – Харків : ХУПС, 2015. – Вип. 5 (130).– С. 129–134. 5. *Свердлик, М.Б.* Оптимальные дискретные сигналы / М.Б.Свердлик. – М. : Сов.радио, 1975. – 200 с. 6. *Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. P. 169 – 178. 7. *Ipatov, Valery P.* Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. – 2005. – 385 p. 8. *Sarvate, D.V.* Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. – 1980. – Vol. Com 68 – P. 59–90. 9. *Gold, R.* Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory.– 1967. – Vol. 13. – P. 619–621. 9. *Замула, А.А.* Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций корреляции / Замула А.А. // Системи обробки інформації. – Харків : ХУПС, 2015. – Вип. 10 (135).– С. 35-39. 10. *Горбенко, И.Д., Замула, А.А., Морозов, В.Л., Семенко, Е.А.* Метод синтеза производных систем сигналов на основе криптографических дискретных последовательностей символов // Радиотехника. – 2017. – Вып. 186. – С. 107 – 116.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 07.10.2017

УДК 681.3.06

А.В. БЕССАЛОВ, д-р техн. наук, О.В. ЦЫГАНКОВА

СУЕПЕРСИНГУЛЯРНЫЕ ПОЛНЫЕ КРИВЫЕ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Введение

Эллиптические кривые в форме Эдвардса над простым полем наиболее перспективны для современных криптосистем. Производительность операции экспоненцирования точки такой кривой в среднем более чем в 1,5 раза выше, чем для кривой в форме Вейерштрасса [1]. Арифметика этих кривых и их программирование существенно упрощаются в связи с наличием нейтрального элемента группы как аффинной точки кривой O = (1,0).

Суперсингулярные эллиптические кривые, интерес к которым был потерян в 90-е годы в связи с уязвимостью к MOV-атаке изоморфизма [2], в начале нынешнего столетия стали основой криптографии на спаривании точек эллиптической кривой [3]. Несомненные технологические преимущества кривых в форме Эдвардса делают актуальной задачу исследования свойств суперсингулярных кривых этого типа.

В настоящей работе дан анализ свойств суперсингулярных кривых одного из классов кривых в обобщенной форме Эдвардса [1] над простым полем – полных кривых Эдвардса. В разд. 1 вводятся основные понятия и определения в соответствии с новой классификацией кривых Эдвардса [1]. В разд. 2 сформулированы и доказаны три теоремы об условиях существования суперсингулярных кривых с j-инвариантами, равными $0,\ 12^3$ и 66^3.

1. Кривые в обобщенной форме Эдвардса и суперсингулярные кривые

В работе [4] *скрученные кривые Эдвардса* (*twisted Edwards curves*) определены как обобщение кривых Эдвардса $x^2 + y^2 = 1 + dx^2y^2$ [5] путем ввода нового параметра a в уравнение

$$\mathrm{E}_{a,d}: ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in \mathrm{F_p}^*,\ d \neq 1,\ a \neq d,\ p \neq 2.$$

Наряду с вводом параметра a авторы [4] сняли ограничения на пару параметров a и d, допуская любые значения $\left(\frac{ad}{p}\right) = \pm 1$. Здесь и далее $\left(\frac{z}{p}\right)$ – символ Лежандра элемента z [3]. При $a = 1$ такая кривая получила в [4] название *кривой Эдвардса*, а если у нее d – квадратичный невычет (т.е. $\left(\frac{d}{p}\right) = -1$), то – *полной кривой Эдвардса*. Этот термин связан с полнотой закона сложения точек кривой [5]. В работе [6] мы предложили поменять местами координаты x и y в форме кривой Эдвардса с целью сохранения горизонтальной симметрии обратных точек, принятой в теории эллиптических кривых. Опираясь на это свойство, определим *кривую в обобщенной форме Эдвардса* уравнением

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2,\ a,d \in \mathrm{F_p}^*,\ d(d-a) \neq 0,\ d \neq 1,\ p \neq 2. \quad (1)$$

Тогда модифицированный универсальный закон сложения точек имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{(1-dx_1x_2y_1y_2)}, \frac{x_1y_2 + x_2y_1}{(1+dx_1x_2y_1y_2)}\right). \quad (2)$$

При совпадении двух точек получим из (2) закон удвоения точек

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{(1-dx_1^2y_1^2)}, \frac{2x_1y_1}{(1+dx_1^2y_1^2)}\right). \quad (3)$$

Определяя теперь обратную точку как $-P = (x_1, -y_1)$, согласно закону (2) получаем координаты нейтрального элемента группы $(x_1, y_1) + (x_1, -y_1) = \mathrm{O} = (1, 0)$. На оси x также всегда лежит точка $D_0 = (-1, 0)$ второго порядка, для которой в соответствии с (3) $2D_0 = (1, 0) = \mathrm{O}$. В зависимости от свойств параметров a и d можно получить еще две особые

точки второго порядка и две особые точки 4-го порядка. Как следует из (1), на оси y могут также лежать не особые точки 4-го порядка $\pm F_0 = (0, \pm 1/\sqrt{a})$, для которых $\pm 2F_0 = D_0 = (-1, 0)$. Эти точки существуют над полем F_p, если параметр a является квадратом (квадратичным вычетом).

Согласно нашей классификации кривых в форме (1), обоснованной в [1, 7, 8], скрученная кривая имеет параметры a и d со свойствами квадратичных невычетов $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right) = -1$, тогда как при $a = 1$ определены полные кривые Эдвардса с параметром d, являющимся квадратичным невычетом $\left(\frac{d}{p}\right) = -1$, и квадратичные кривые Эдвардса, для которых $\left(\frac{d}{p}\right) = 1$. Полные кривые Эдвардса являются циклическими в отношении точек четных порядков и не содержат особых точек. Важно, что нециклические скрученные и квадратичные кривые Эдвардса образуют пары квадратичного кручения, параметры которых связаны линейным преобразованием $a' = ca, d' = cd$, где $\left(\frac{c}{p}\right) = -1$ [1,8]. Этим свойством удобно пользоваться при анализе суперсингулярных кривых этих классов, для которых можно принять $a = 1$ и ограничиться одним параметром со свойством $\left(\frac{d}{p}\right) = 1, d \neq 1$. Другими словами, анализ суперсингулярных кривых двух классов – скрученных и квадратичных кривых Эдвардса – сводится к анализу последних с одним параметром d.

Порядок N_E эллиптической кривой над конечным полем $F_q, q = p^m$ определяется на основе следа уравнения Фробениуса t как $N_E = q + 1 - t$. Для кривой квадратичного кручения E^t соответствующий порядок будет $N_E^t = q + 1 + t$. Эллиптическая кривая является суперсингулярной тогда и только тогда, когда над любым расширением простого поля F_p след $t \equiv 0 mod p$. [3]. Иными словами, в алгебраическом замыкании $\overleftarrow{F_p}$ суперсингулярная кривая не содержит точек порядка p. Над простым полем F_p такая кривая всегда имеет порядок $N_E = p + 1$, а над любым расширением этого поля $N_E \equiv 1 mod p$.

Для кривой

$$E: \quad Y^2 = X^3 + AX + B \tag{4}$$

в канонической форме Вейерштрасса с j-инвариантом [3, 9]

$$j(E) = \frac{12^3\, 4A^3}{4A^3 + 27B^2} \tag{5}$$

характерными являются значения $j(E) = 0$ при $A = 0$ и $j(E) = 12^3$ при $B = 0$. Эти значения j-инварианта часто (но не всегда) порождают суперсингулярную кривую.

Изоморфизм кривых в формах (1) и (4) достигается лишь приблизительно для четверти всех кривых в форме Вейерштрасса, содержащих одну или три точки 2-го порядка. Порядок таких кривых $N_E \equiv 0 mod 4$. Наиболее удобной формой их представления является кривая в форме Монтгомери [4]

$$E_{C,D}: \quad Dv^2 = u^3 + Cu^2 + u, C = 2\frac{a+d}{a-d}, D = \frac{4}{a-d}, a = \frac{C+2}{D}, d = \frac{C-2}{D}, \tag{6}$$

$$C^2 \neq 4.$$

Как частный случай канонической кривой (4) в форме Вейерштрасса, уравнение (6) часто используется при анализе свойств кривой в обобщенной форме Эдвардса (1). Так как кривые (1) и (6)) изоморфны ($E_{a,d} \sim E_{C,D}$) [1, 4], доказательства условий существования таких суперсингулярных кривых равнозначны.

Для кривой (1) j-инвариант [10]

$$j(a, d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, ad(a - d) \neq 0. \tag{7}$$

Так как j-инвариант сохраняет свое значение для всех изоморфных кривых и пар квадратичного кручения [3], он является полезным инструментом при поиске суперсингулярных кривых. Как отмечалось, для этих целей параметр a в (7) является избыточным, т.е. можно принять $a = 1$ и рассматривать свойства лишь полных и квадратичных кривых Эдвардса. Если квадратичная кривая – суперсингулярная, то и соответствующая ей скрученная кривая (как пара квадратичного кручения) – также суперсингулярная. В этой связи в дальнейшем принимаем $a = 1$ и будем пользоваться j-инвариантом $j(1, d)$.

Одним из свойств j-инварианта является

$$j(1, d) = j(1, d^{-1}). \tag{8}$$

Это свойство легко доказать, обращая элемент d в (7) и умножая числитель и знаменатель на d^6, после чего можно получить равенство (8). Как известно, обращение параметра $d \to d^{-1}$ дает кривую квадратичного кручения для полной кривой Эдвардса [5], и изоморфную – для квадратичной кривой Эдвардса [1].

2. Необходимые условия существования суперсингулярных полных кривых Эдвардса

Порядок кривых Эдвардса $N_E \equiv 0 mod 4$, тогда суперсингулярные кривые в форме Эдвардса с порядком $N_E = p + 1$ существуют лишь при $p \equiv 3 mod 4$. Поэтому в данной работе рассматриваем лишь этот случай как первое необходимое условие существования суперсингулярных кривых этого класса.

Полная кривая Эдвардса определена в работах [4, 5] как частный случай кривой (1):

$$\mathrm{E}_{1,d}: \quad x^2 + y^2 = 1 + dx^2y^2 \,,\ d \in \mathrm{F_p}^*,\ d(d-1) \neq 0,\ \left(\frac{d}{p}\right) = -1 \tag{9}$$

Характерными свойствами этого класса кривых являются цикличность группы точек четного порядка и отсутствие особых точек (или полнота закона сложения точек) [5].

2.1. Суперсингулярные полные кривые Эдвардса с нулевым j-инвариантом

Такие кривые изоморфны подклассу кривых (4) в форме Вейерштрасса вида $Y^2 = X^3 + B$ с j-инвариантом (5), равным 0. Хотя любая кривая этого вида имеет нулевой j-инвариант, не все они являются суперсингулярными. Кроме того, не любая из этих кривых сводится к форме Монтгомери (6).

Теорема 1. *При* $p \equiv -1 mod 12$ *полная кривая Эдвардса над простым полем с нулевым j-инвариантом* и *с параметрами* $d_{1,2} = -7 \pm 4\sqrt{3}$, *является суперсингулярной.*

Доказательство. При нулевом значении j-инварианта (7) решения для параметра d кривой определяются корнями квадратного уравнения $d^2 + 14d + 1 = 0$

$$d_{1,2} = -7 \pm 4\sqrt{3}, d_1 d_2 = 1. \tag{10}$$

Отсюда следует, что кривые с нулевым j-инвариантом существуют лишь при существовании элемента простого поля $\sqrt{3}$. Элемент 3 является квадратичным вычетом при $p \equiv \pm 1 mod 12$ [11]. При $p \equiv 1 mod 12$ имеет место сравнение $p \equiv 1 mod 4$, при этом кривые Эдвардса несуперсингулярны. Итак, в условиях теоремы кривая с параметрами (10) имеет нулевой инвариант $j(1, d) = 0$.

Докажем, что порядок кривой в условиях теоремы $N_E = p + 1$. Сначала покажем, что при выполнении сравнения $p \equiv -1 mod 12$ выполняется и условие $p \equiv 3 mod 4$. Действительно, из $p = 12k - 1$ следует $p \equiv -1 mod 4 = 3 mod 4$. Далее, любая кривая с нулевым j-инвариантом (5) изоморфна кривой (4) вида $Y^2 = X^3 + B$. При выполнении условия $p \equiv -1 mod 12$ теоремы также справедливо сравнение $p \equiv -1 mod 3 \equiv 2 mod 3$, тогда порядок $(p - 1)$ мультипликативной группы поля не делится на 3. При этом группа не

содержит подгруппы (и, соответственно, элементов) 3-го порядка и НОД$(p-1,3)=1$ [12]. Если $g-$ примитивный элемент мультипликативной группы поля F_p, то и g^3 – также примитивный элемент. В уравнении $Y^2=X^3+B$ для всех $X=0\ldots(p-1)$ правая часть уравнения при любом B пробегает все те же значения. Из них $\frac{p-1}{2}$ квадратичных вычетов, которые дают ровно $(p-1)$ точек кривой, элемент 0 из множества значений X^3+B дает одну точку 2-го порядка, тогда с добавлением точки на бесконечности получаем порядок кривой $N_E=p+1$. Подчеркнем, что данная кривая циклическая с одной точкой 2-го порядка и двумя точками 4-го порядка (т.к. при $p\equiv 3mod4$ имеет место $4|(p+1)$), и, следовательно, она изоморфна полной кривой Эдвардса, при этом все корни в (10) – квадратичные невычеты. Таким образом, в условиях теоремы кривая (1), изоморфная кривой в форме Вейерштрасса $Y^2=X^3+B$, имеет порядок $N_E=p+1$ и, следовательно, является суперсингулярной.

Если в уравнении $Y^2=X^3+B$ принять $B=-e^3$ и $u=X-e$, можно получить изоморфную кривой (4) кривую (6) в форме Монтгомери вида

$$y^2=u^3+3eu^2+3e^2u.$$

Делением на $(\sqrt{3}e)^3$ она приводится к виду (6)

$$v^2=u^3+\sqrt{3}u^2+u.$$

Тогда с учетом уравнения (6) из равенства $2\frac{1+d}{1-d}=\sqrt{3}$ получаем

$$d=\frac{\sqrt{3}-2}{\sqrt{3}+2}$$

и два решения для этого параметра

$$d_{1,2}=\left(\frac{\sqrt{3}-2}{\sqrt{3}+2}\right)^{\pm 1}.$$

Эти значения совпадают с решениями (10), в чем можно убедиться умножением числителя и знаменателя d_1 на $\left(\sqrt{3}-2\right)$, тогда $.-\left(\sqrt{3}-2\right)^2=-7+4\sqrt{3}$. Аналогично получаем и второе решение для инверсии ${d_1}^{-1}$. В произведении $\left(\sqrt{3}+2\right)\left(\sqrt{3}-2\right)=-1$ один из сомножителей – квадратичный вычет, другой – квадратичный невычет, так как $p\equiv 3mod4$ и $\left(\frac{-1}{p}\right)=-1$ [9]. Это доказывает, что параметры (10) – квадратичные невычеты и кривая входит в класс полных кривых Эдвардса. Теорема доказана. ▲

В табл. 1 в качестве примера приведены значения p в первой сотне чисел, для которых справедливы условия теоремы, вместе со взаимно обратными значениями $d_{1,2}$, вычисленными согласно (10). Они определяют все суперсингулярные полные кривые Эдвардса с нулевым j-инвариантом и порядком $N_E=p+1$.

Таблица 1

p	11	23	47	59	71	83
$d_{1,2}$	(2, 6)	(11,21)	(39,41)	(8,37)	(23,34)	(24,45)

Все полные кривые Эдвардса с нулевым j-инвариантом при $p\equiv 1mod12$ (при этом $p\equiv 1mod4$) являются несуперсингулярными. Это очевидно, так как в этом случае $(p+1)$ не делится на 4.

2.2. Суперсингулярные полные кривые Эдвардса с j-инвариантом $j(1,d)=12^3$

Приведем условия существования суперсингулярных кривых этого класса.

Теорема 2. *При* $p\equiv 3mod4$ *полная кривая Эдвардса над простым полем с j-инвариантом* $j(1,d)=12^3$ и *с параметром* $d=-1$ *является суперсингулярной.*

Доказательство. Для кривой в форме Вейерштрасса (4) вида $Y^2=X^3+AX$ $(B=0)$ согласно (5) получаем $j(E)=12^3$. Изоморфизм с полной кривой Эдвардса здесь существует лишь в случае, если $A=G^2$, тогда кривая (4) сводится к форме Монтгомери (6). Разделим правую часть уравнения (4) при $B=0$ на G^3, тогда после замены $\frac{X}{G}\to u, \frac{Y}{G}\to v$ приходим к кривой (6) вида $Dv^2=u^3+Cu^2+u$, при этом $C=2\frac{1+d}{1-d}=0$. Отсюда следует, что $1+d==0, \Rightarrow d=-1$. Это значение есть квадратичный невычет при $p\equiv 3mod4$ [9], и изоморфная кривой (6) кривая (1) – полная кривая Эдвардса.

С другой стороны, суперсингулярные кривые над простым полем со следом Фробениуса $t=0$ изоморфны своему квадратичному кручению: $E\sim E^t$. Переход к кривой кручения в классе полных кривых Эдвардса $x^2+y^2=1+dx^2y^2, \left(\frac{d}{p}\right)=-1,$ достигается, как отмечалось, обращением параметра $d\to d^{-1}$ [5]. Тривиальным примером суперсингулярной кривой в этом классе является значение $d=d^{-1}=-1$, найденное выше для кривой в форме Монтгомери. В этом случае пара квадратичного кручения вырождается в одну кривую, след Фробениуса $t=0$ и порядок кривой $N_E=p+1$. Теорема доказана. ▲

Для пары $(1,d)=(1,-1)$ согласно (7) получим

$$j(1,d)=\frac{16(-12)^3}{-4^2}=12^3.$$

Заметим, что кривая (4) при $B=0$ может оказаться нециклической (с тремя точками 2-го порядка), но всегда является суперсингулярной при $p\equiv 3mod4$ [9].

В общем случае для нахождения кривой Эдвардса с j-инвариантом $j(1,d)=12^3$ в соответствии с (7) следует решить уравнение 6-й степени:

$$\frac{16(1+d^2+14d)^3}{d(1-d)^4}=12^3\Rightarrow(1+d^2+14d)^3-2^23^3\,d(1-d)^4=0. \qquad (11)$$

Уравнение (11) может дать до шести корней или три пары взаимно-обратных значений $d_i^{\pm1}, i=1,2,3$. Пары корней, являющихся квадратичными невычетами, отвечают полной кривой Эдвардса, в противном случае – квадратичной кривой. Как следует из приведенного анализа, существует единственная полная кривая Эдвардса с j-инвариантом $j(1,d)=12^3$ при $d=-1$ (этот корень уравнения (11) имеет кратность 2).

Значениями $j(1,d)=0,12^3$ не исчерпываются все суперсингулярные кривые. В работах [1, 6] мы обнаружили и привели доказательство теоремы об условии существования полной суперсингулярной кривой с параметрами $d=2^{\pm1}$. Здесь дадим новое строгое доказательство этой теоремы.

2.3. Суперсингулярные полные кривые Эдвардса с j-инвариантом $j(1,d)=66^3$

Принимая $x,y\neq 0,1$, разделим уравнение (9) на x^2y^2, тогда получим

$$E_{1,d}\colon (y^{-2}-1)(x^{-2}-1)=1-d\Rightarrow y^{-2}-1=\frac{1-d}{x^{-2}-1}, x,y\neq 0,1 \qquad (12)$$

Иногда это уравнение удобней записать в форме

$$y^{-2}=\frac{x^{-2}-d}{x^{-2}-1}, x,y\neq 0,1.$$

Для квадратичной кривой Эдвардса отсюда сразу определяются координаты особых точек $x^{-2}=d, y^{-2}=d$.

После исключения четырех базовых точек $O, D, \pm F$ $(x, y \neq 0,1)$ суперсингулярные кривые следует искать на основе нахождения числа решений уравнения (12) со значениями параметра $d^{\pm 1}$, дающими одинаковое число решений (это справедливо для полных кривых, у которых замена $d \to d^{-1}$ дает пару квадратичного кручения [5]).

Уравнение (12) можно использовать для поиска параметров d суперсингулярных кривых, для которых подмножества левой и правой части уравнения, включающие квадратичные вычеты и невычеты, пересекаются, т.е. содержат одинаковые элементы. Такой подход требует изучения свойств множества $\{x^{-2} - 1\}$ с учетом структуры полных кривых Эдвардса (без особых точек) и квадратичных кривых Эдвардса (с особыми точками 2-го и 4-го порядков). В данной работе мы рассматриваем лишь первый класс этих кривых. Подобный же анализ для квадратичных и скрученных кривых Эдвардса мы дадим в следующей работе.

Обозначим множество всех элементов в знаменателе (12) как

$$U = \{u^{-2} = x^{-2} - 1, x = 2,3, \dots, \tfrac{(p-1)}{2}\}. \quad (13)$$

Мощность этого множества $|U| = \frac{(p-3)}{2}$.

Пусть

$$Q_p = \{1^2, 2^2, 3^2, \dots \left(\tfrac{(p-1)}{2}\right)^2\} -$$

множество всех ненулевых квадратов, и, соответственно, $\overline{Q_p}$ – множество всех квадратичных невычетов. При $p \equiv 3 mod 4$, очевидно, $\overline{Q_p} = -Q_p$.

Множество U (13) является суммой непересекающихся подмножеств квадратичных вычетов из множества Q_p

$$S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3, \dots, \tfrac{(p-1)}{2}\} \quad (14)$$

и невычетов

$$\bar{S} = \{u^{-2} = (x^{-2} - 1) \in \overline{Q_p}, x = 2,3, \dots, \tfrac{(p-1)}{2}\} \quad (15)$$

с элементами из множества $\overline{Q_p}$ квадратичных невычетов. Мы рассматриваем множества как наборы элементов поля F_p, вычисленных при различных значениях $x, y \neq 0,1$.

Для доказательства теоремы нам потребуются доказать следующие леммы.

Лемма 1. *При p* ≡ 3mod4 *мощности множеств ненулевых квадратов*

$$S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3, \dots, \tfrac{(p-1)}{2}\}$$

и квадратичных невычетов

$$\bar{S} = \{u^{-2} = (x^{-2} - 1) \in \overline{Q_p}, x = 2,3, \dots, \tfrac{(p-1)}{2}\}$$

одинаковы и равны $|S| = |\bar{S}| = \frac{(p-3)}{4}$.

Доказательство. Число решений уравнения $u^{-2} = x^{-2} - 1$ определяется числом квадратов в правой части. Подобная задача была рассмотрена в работе [13]. Согласно лемме 2 этой работы при p ≡ 3mod4 число ненулевых квадратичных вычетов в множестве элементов $\{(x^{-2} - 1), x = 1,2,3, \dots, \frac{(p-1)}{2}\}$, равно $(p - 3)/4$. При $x = 1$ получаем $(x^{-2} - 1) = 0 -$ элемент, не входящий в число вычетов, поэтому число ненулевых квадратичных вычетов u^{-2} равно $(p - 3)/4$. Так как по условию $x \neq 1$, то множество всех элементов $\{x^{-2} - 1\}$ мощности $(p - 3)/2$ содержит равное число $(p - 3)/4$ квадратичных вычетов и невычетов, т.е. $|S| = |\bar{S}| = \frac{(p-3)}{4}$. Лемма доказана.

Очевидно, что утверждение леммы инвариантно к замене $x^{-2} \to x^2$.

Лемма 2. *При* $p \equiv 3\mathrm{mod}8$ *множество ненулевых квадратов* $S = \{u^{-2} = (x^{-2} - 1) \in Q_p, x = 2,3,\dots,\frac{(p-1)}{2}\}$ и множество квадратичных невычетов $-S = \{-u^{-2} = (1 - x-2) \in Qp\ x=2,3,\dots, p-12\}$ содержат *ровно по* $(p-3)8$ *пар взаимно-обратных элементов.*

Доказательство. Пусть для некоторого $z^2 \neq x^2$ существует элемент из множества $\{u^{-2} = x^{-2} - 1\}$, такой, что $(z^{-2} - 1)(x^{-2} - 1) = 1$. Тогда элементы $((z^{-2} - 1), (x^{-2} - 1)) \in S$ взаимно-обратны. Уравнение для z^{-2} можно записать как

$$z^{-2} - 1 = \frac{1}{x^{-2}-1},$$

или

$$z^{-2} = \frac{x^{-2}}{x^{-2}-1} \Rightarrow z^2 = 1 - x^2, x, z \neq 0,1. \quad (16)$$

Согласно лемме 1 число решений этого уравнения для всех $x = 2,3,\dots,\frac{(p-1)}{2}$ равно $(p - 3)/4$. При $p \equiv 3\mathrm{mod}8$ для каждого квадрата из множества квадратов S найдется элемент $(z^{-2} - 1)$ этого множества, обратный первому. Так как при $p \equiv 3\mathrm{mod}8$ элемент $2 \in \overline{Q_p}$ [9], то $x^{-2} \neq 2$ и $x^{-2} - 1 \neq 1$. Другими словами, множество S не содержит 1. Таким образом, множество S в условиях леммы включает ровно $(p - 3)/8$ пар взаимно-обратных элементов. В множестве $-S$ все квадратичные вычеты множества S становятся невычетами с сохранением свойства обратимости (но уже только для квадратичных невычетов) и числа элементов. Лемма доказана.

Лемма 3. *При* $p \equiv 3\mathrm{mod}8$ *подмножество* $\bar{S}$ *множества* U *не содержит пар взаимно-обратных элементов.*

Доказательство. Допустим обратное, и справедливо уравнение (16) для квадратичных невычетов подмножества $\bar{S}$. Тогда

$$z^{-2} = \frac{x^{-2}}{x^{-2}-1} \Rightarrow \left(\frac{z}{x}\right)^{-2} = \frac{1}{x^{-2}-1}. \quad (17)$$

Правая часть равенства согласно допущению есть квадратичный невычет, а левая – квадрат. Для половины квадратов множества $S = \{x^{-2} - 1\}$ дает согласно лемме 2 $\frac{(p-3)}{8}$ решений, тогда как для половины невычетов $\bar{S}$ таких решений нет. Следовательно, все элементы в подмножестве $\bar{S}$ необратимы (т.е. $\bar{S}$ не содержит пар мультипликативно обратных элементов). Лемма доказана.

С другой стороны, если допустить обратимость элементов $\bar{S}$, то вместе с обратимостью элементов S это даст $(p - 3)/2$ решений уравнения (12) и $2(p - 3)$ точек кривой, что невозможно.

Лемма 4. *При* $p \equiv 3\mathrm{mod}8$ *множества* $U = \{u^{-2} = x^{-2} - 1, x = 2,3,\dots,\frac{(p-1)}{2}\}$ *и* $-U$ *содержат по* $(p - 3)/8$ *одинаковых квадратичных вычетов и невычетов, и мощность их пересечения равна* $(p - 3)/4$.

Доказательство. Обозначим пересечение множеств U и $-U$ как $V = U * (-U)$. Тогда оно имеет подмножества S_v квадратичных вычетов и $\overline{S_v}$ квадратичных невычетов, причем $V = S_v + \overline{S_v}$. Одинаковые элементы этих множеств определяются из равенства

$$x^{-2} - 1 = 1 - z^{-2} \Rightarrow z^{-2} = 2 - x^{-2}, x = 2,3,\dots,\frac{(p-1)}{2}.$$

Как и в лемме 1, это уравнение имеет $(p - 3)/4$ решений [13], а множество $\{1 - z^{-2}\} = -U$ является суммой подмножеств квадратов $-\bar{S}$ и квадратичных невычетов $-S$ равной мощности $(p - 3)/8$. Это следует из того, что множество U также содержит два непересекающихся подмножества S и $\bar{S}$ с числом элементов по $(p - 3)/8$. Таким образом, ровно половина всех квадратов S множества U и невычетов $\bar{S}$ этого множества совпадают с

соответствующими подмножествами множества $-U$, при этом $|S_v| = |\overline{S_v}| = (p - 3)/8$. Тогда общее число совпадающих элементов этих множеств $|V| = |U * (-U)| = (p - 3)/4$. Это доказывает утверждение леммы.

Лемма 5. *При $p \equiv 3 mod 8$ для каждой пары взаимно-обратных квадратов $u^{\pm 2}$ множества S существует единственный элемент множества невычетов $\bar{S}$, равный $-u^2$ или $-u^{-2}$.*

Доказательство. Как следует из леммы 2, множества вычетов S и невычетов $-S$ состоят из $\frac{(p-3)}{8}$ пар взаимно-обратных элементов. Вместе с тем, согласно лемме 4 множества невычетов $\bar{S}$ и $-S$ пересекаются лишь наполовину и содержат $\frac{(p-3)}{8}$ одинаковых элементов. Требуется доказать, что из каждой пары взаимно-обратных элементов множества $-S$ лишь один элемент попадает в множество $\bar{S}$.

Пусть $u_1^{\pm 2} = (x_1^{-2} - 1)^{\pm 1}$ – пара квадратов множества S. Предположим, что существует квадратичный невычет $u_2^{-2} = (x_2^{-2} - 1) \in \bar{S}$, такой, что справедливо

a) $(x_2^{-2} - 1) = -u_1^{-2} = (1 - x_1^{-2}) \Rightarrow x_2^{-2} = (2 - x_1^{-2})$

b) $(x_2^{-2} - 1) = -u_1^{2} = (1 - x_1^{-2})^{-1} \Rightarrow x_2^{-2} = \frac{(2 - x_1^{-2})}{(1 - x_1^{-2})}$

Поскольку при $p \equiv 3 mod 8$, элемент $2 \in \overline{Q_p}$ [12], правая часть равенств a) и b) не равна 0 (это тождественно отсутствию особых точек деления на 0 у полной кривой Эдвардса (12) при $d = 2^{\pm 1}$). По условию элемент $(1 - x_1^{-2})$ является квадратичным невычетом. Отсюда ясно, что существует единственное решение для невычета $-u_1^{-2}$ или $-u_1^2$ множеств $\bar{S}$ и $-S$, так как при выполнении равенства a) не выполняется равенство b), и наоборот. Лемма доказана.

Теорема 3. *При $p \equiv 3 mod 8$ полная кривая Эдвардса над $\mathbf{F}_p$ с параметрами $d = 2^{\pm 1}$ является суперсингулярной.*

Доказательство. Из сравнения $p \equiv 3 mod 8$ сразу следует $p \equiv 3 mod 4$, так как редукция первого сравнения $8k + 3, k = 1,2, \ldots$, по модулю 4 дает второе. Следовательно, $4|(p + 1)$ и порядок кривой делится на 4. При выполнении сравнения $p \equiv 3 mod 8$ элемент 2 поля F_p является квадратичным невычетом, т.е. $\left(\frac{2}{p}\right) = -1$ [12], тогда при $d = 2^{\pm 1}$ имеем полную кривую Эдвардса. Требуется доказать, что при $d = 2$ порядок кривой (9) равен $p + 1$ и кривая суперсингулярная.

При $d = 2$ уравнение (12) имеет вид

$$y^{-2} - 1 = \frac{1}{1 - x^{-2}}, x = 2,3, \ldots, \frac{(p-1)}{2}. \quad (18)$$

Как следует из леммы 1, одинаковые множества $U = \{y^{-2} - 1\}$ и $\{x^{-2} - 1\}$ содержат по $\frac{(p-3)}{4}$ квадратичных вычетов и невычетов, что составляет ровно половину всех вычетов (без элемента 1) и невычетов (без элемента -1). В соответствии с (18) надо найти число совпадающих элементов множества U и множества обратных элементов $-U^{-1} = \{u^2 = (1 - x^{-2}), x = 2,3, \ldots, \frac{(p-1)}{2}\}\}$.

Свойства множеств квадратов S и квадратичных невычетов $\bar{S}$ (леммы 2 и 3) сводятся к тому, что множество S состоит из $\frac{(p-3)}{8}$ пар $u^{\pm 2}$ взаимно-обратных квадратов, тогда как множество $\bar{S}$ не содержит таких пар.

Лемма 4 утверждает, что пересечение множеств U и $-U$ содержит подмножества S_v квадратичных вычетов и $\overline{S_v}$ квадратичных невычетов с мощностями $|S_v| = |\overline{S_v}| = (p - 3)/8$. Тогда согласно лемме 5 для каждой пары квадратов $u_1^{\pm 2} \in S$ существует единственный квадратичный невычет из пары $-u_1^{\pm 2}$, который принадлежит множеству квадратичных невычетов $\bar{S}$.

С учетом этих свойств существует одно из двух альтернативных подмножеств $G_1 \in U$ или $G_1^* \in U$ из четырех элементов

$$G_1 = \{u_1^{-2}, u_1^2, -u_1^{-2}, -u_2^{-2}\} \in U, \quad (19)$$

$$G_1^* = \{u_1^{-2}, u_1^2, -u_1^2, -u_2^{-2}\} \in U, \quad (20)$$

из которых первые два являются парой взаимно-обратных квадратов, а последние – парой необратимых квадратичных невычетов $(u_1^{\pm 2} * u_2^{-2} \neq 1)$. Необратимость последних невычетов следует из леммы 3. Последний элемент в (19) или (20) может быть любым отличным от первого невычетом множества $\bar{S}$. Умножая все его элементы на -1 и обращая каждый из них, получим одно из подмножеств

$$-G_1{}^{-1} = \{-u_1^2, -u_1^{-2}, u_1^2, u_2^2\} \in -U^{-1},$$

$$(-G_1^*)^{-1} = \{-u_1^2, -u_1^{-2}, u_1^{-2}, u_2^2\} \in -U^{-1}.$$

Отсюда следует, что их пересечение с подмножествами соответственно (19) и (20) имеет две альтернативы:

$$G_1 * (-G_1{}^{-1}) = \{u_1^2, -u_1^{-2}\}, \text{ или } G_1^* * (-G_1^*)^{-1}) = \{u_1^{-2}, -u_1^2\}.$$

Каждая из них содержит ровно два элемента, один из которых – квадратичный вычет, а другой – невычет. Так как все множество U согласно лемме 2 содержит $\frac{(p-3)}{8}$ пар взаимно-обратных квадратов, то можно построить то же число его подмножеств G_1 (или G_1^*), элементы которых определены подмножествами (19) или (20). Тогда мощность пересечения двух множеств U и $(-U)^{-1}$

$$|U * (-U)^{-1}| = \frac{(p-3)}{4}.$$

Итак, имеется ровно $\frac{(p-3)}{4}$ решений уравнения (18), из которых половину решений дают квадратичные вычеты, половину – невычеты. Так как каждое решение уравнения (18) дает по четыре точки $(\pm x, \pm y)$ кривой (9), получаем $(p-3)$ точек, удовлетворяющих уравнению (18). Добавляя четыре отброшенные при анализе точки O = (1, 0), D = (– 1, 0) и $\pm F = (0, \pm 1)$, получаем при $d = 2$ порядок кривой (9) $N_E = p + 1$. Такая кривая является суперсингулярной со следом Фробениуса $t = 0$, поэтому пара квадратичного кручения с параметром $d = 2^{-1}$ имеет тот же порядок. Теорема доказана. ▲

Пример. При $p = 19 \equiv 3 \bmod 8$ в табл. 2 представлены элементы всех множеств, используемых в теореме 3.

Таблица 2

x^{-1}	2	3	4	5	6	7	8	9
x^{-2}	4	9	16	6	17	11	7	5
$U = \{u^{-2} = x^{-2} - 1\}$	3	8	15	5	16	10	6	4
S				5	16		6	4
$\bar{S}$	3	8	15			10		
$-U$	16	11	4	14	3	9	13	15
$-U^{-1}$	6	7	5	15	13	17	3	14
$-S$	16	11	4			9		
$-\bar{S}$				14	3		13	15
$V = U * (-U)$	16		4		3			15
S_v	16		4					
$\bar{S_v}$					3			15
$U * (-U)^{-1}$	3		15	5			6	

Здесь два подмножества (19) или (20) можно построить как

$$G_1 = \{4, 5, -u_1^{-2} = 15, -u_2^{-2} = 10\},$$
$$G_1^{'} = \{16, 6, -u_1^{-2} = 3, -u_2^{-2} = 8\}.$$

Тогда

$$-G_1 = \{15, 14, u_1^{-2} = 4, u_2^{-2} = 9\} \Rightarrow (-G_1)^{-1} = \{14, 15, 5, 17\},$$
$$-G_1^{'} = \{3, 13, u_1^{-2} = 16, u_2^{-2} = 11\} \Rightarrow (-G_1^{'})^{-1} = \{13, 3, 6, 7\},$$

а пересечения соответствующих подмножеств включают элементы:

$$G_1 * (-G_1)^{-1} = \{5, 15\},$$
$$G_1^{'} * (-G_1^{'})^{-1} = \{6, 3\}.$$

Итак, получены $\frac{(p-3)}{4} = 4$ решения уравнения (18), причем два из них – для квадратичных вычетов, и два – для невычетов, что отвечает теореме 3. Приведенный пример дает наиболее простую иллюстрацию схемы доказательства.

При $d = 2^{\pm 1}$ j-инвариант (7) полной суперсингулярной кривой Эдвардса равен $j(1,2) = 2^3 \cdot 3^3 \cdot 11^3 = 66^3$.

При $x, y \neq 0,1$ уравнения кривой (12) при $d = 2^{\pm 1}$ для пары квадратичного кручения имеют вид:

$$E_{1,d}: (y^{-2} - 1) = \frac{-1}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2},$$
$$E_{1,d}^{t}: (y^{-2} - 1) = \frac{2^{-1}}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2}. \quad (21)$$

Так как элементы (–1) и 2 – квадратичные невычеты, то в соответствии с леммой 1 в правой части уравнений имеется равное число $\frac{(p-3)}{4}$ квадратичных вычетов и невычетов. Такое же соотношение их для левых частей уравнений. Из доказанной теоремы 3 следует, что при $p \equiv 3 \bmod 8$ ровно половина всех квадратичных вычетов множеств в левой и правой части этих уравнений совпадают. Такое же утверждение справедливо для квадратичных невычетов.

Интересно заметить, что для суперсингулярной кривой с параметром $d = -1$ и j-инвариантом $j(1, -1) = 12^3$ два уравнения (12) для пары квадратичного кручения вырождаются в одно уравнение

$$E_{1,d}: (y^{-2} - 1) = \frac{2}{(x^{-2} - 1)}, x = 2,3, \dots, \frac{(p-1)}{2},$$

совпадающее с (21) после замены $2 \rightarrow 2^{-1}$.

Существуют ли другие суперсингулярные полные кривые Эдвардса, кроме рассмотренных выше? Вопрос открытый. Пока нам удалось установить с помощью вычислений на компьютере, что в первой сотне значений модуля p других кривых этого класса не существует.

Список литературы: 1. *Бессалов А.В.* Эллиптические кривые в форме Эдвардса и криптография: монография / А.В. Бессалов – Киев : Политехника, 2017. – 272с. 2. *Menezes A.J, Okamoto T., Vanstone S. A.* Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. University of Waterloo, sep. 1990. And // IEEE Transactions on Information Theory, V39, 1993. – PP 1639-1646. 3. *Washington L. C.* Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008. 4. *Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane.* Twisted Edwards Curves. IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17. 5. *Bernstein Daniel J., Lange Tanja.* Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007).

Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50. 6. *Бессалов А.В., Цыганкова О.В.* Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем // Проблемы передачи информации. – 2015. – Т. 51, вып 4. – С.92-98. 7. *Бессалов А.В., Цыганкова О.В.* Классификация кривых в форме Эдвардса над простым полем. Прикладная радиоэлектроника. – 2015. – Т. 14. №4. – С.197 – 203. 8. *Бессалов А.В., Цыганкова О.В.* Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой // Проблемы передачи информации. – 2017. – Т.53, вып 1. – С.101-111. 9. *Бессалов А.В., Телиженко А.Б.* Криптосистемы на эллиптических кривых : учеб. пособие. – К. : Політехніка, 2004. – 224с. 10. *Morain F.* Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009. 11. *Дэвенпорт Г.* Высшая арифметика: введение в теорию чисел ; пер. с англ. под ред. Ю.В. Линника. – М. : Наука, 1965. – 176с. 12. *Ковальчук Л.В., Беспалов О.Ю, Огнєв П.І.* Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків // Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Вип.1(25). – С.58 – 67. 13. *Бессалов А.В., Ковальчук Л.В.* Точное число эллиптических кривых в канонической форме, изоморфных кривым Эдвардса над простым полем // Кибернетика и системный анализ. – 2015. – Т.51, №2. – С.3-12.

Национальный технический университет «КПИ» *Поступила в редколлегию 04.11.2017*

УДК 004.652

В.И. ЕСИН, д-р техн. наук

ВЫРАЗИТЕЛЬНЫЕ СРЕДСТВА МОДЕЛИ ДАННЫХ «ОБЪЕКТ-СОБЫТИЕ»

Введение

В моделировании данных их представление является важной задачей, от решения которой существенно зависит взаимопонимания между участниками процесса создания базы данных (БД): аналитиками, разработчиками, специалистами предметной области (ПрО), программистами. В случае расхождения языка формализации, как выразительного средства для представления результата концептуального моделирования – концептуальной модели (схемы) ПрО, со складом мышления специалиста, реализация БД, как отмечается в работе [1], может стать слишком сложной или вообще неразрешимой проблемой.

Используя, например, множества понятий, отношения $\mathbb{R}$ и функции $\mathbb{F}$, определяющие совокупность правил структурирования данных ПрО, множество ограничений целостности P модели данных «объект-событие» [2, 3], можно адекватно описать рассматриваемую предметную область, представив ее интенсионал и экстенсионал в предикатной форме. Для этого с каждым отношением, подобным приведенным в работах [2, 3], вида $R_i(A_{i1},...,A_{ik})$, необходимо сопоставить предикат $R_i(x_{i1},...,x_{ik})$, переменные которого $x_{i1},...,x_{ik}$ имеют те же сорта, что и $A_{i1},...,A_{ik}$ (атрибуты отношения R_i). После чего заменить эти предикаты (элементарные формулы) множеством соответствующих атомарных формул $R_i(c_{i1},...,c_{ik})$, где для кортежа констант ($c_{i1},...,c_{ik}$) выполнимо равенство $R_i(c_{i1},...,c_{ik}) = true$.

Однако, несмотря на то, что данный подход имеет значительную теоретическую проработку, для неподготовленного специалиста такая теоретико-множественная модель с ограничениями, сформулированными с помощью выражений математической логики, достаточно сложна для восприятия и понимания. Хотя при определенных преобразованиях этот подход к формализации ПрО также становится востребованным и используемым. А именно, в модели данных с универсальным базисом отношений, которая является результатом отображения модели «объект-событие» в даталогическую среду и рассматривается в работах [4 – 6].

Поэтому, опираясь на результаты анализа публикаций в различных авторитетных изданиях, посвященных вопросам семантического моделирования [7 – 12], в которых констатируется предпочтение использования графического представления данных, как лучше и быстрее усваиваемое участниками проекта («a picture is worth a thousand words» [7]), были разработаны выразительные средства (так называемые [9, 10], языки концептуального моделирования) для представления концептуальных моделей ПрО в графическом виде, основанные на модели данных «объект-событие» и являющиеся ее составными элементами.

Представление концептуальной схемы предметной области в виде диаграммы модели «объект-событие»

Моделирование ПрО в рассматриваемом подходе базируется на использовании разработанного выразительного средства как системы определенных графических обозначений (знаков), включающих ограниченное число разнородных компонентов (элементов нескольких основных типов) и правил их описания. Типы компонентов этого средства, являющиеся графическим отображением основных понятий модели данных «объект-событие»:

$$\mathfrak{A} = \{\text{Раздел, КлассО, ТипО, ЭкзО, ТипХОф, ТипХОп, ЗначХО, КлассПО, ТипХПО, ЗначХПО, КлассС, ЭкзС, ТипХС, ЗначХС, Документ, Папка, ЕдИзмер}\}$$

(табл. 1) и отношений между ними (рис. 1) в виде определенных геометрических фигур и уточняющей внутри них информации, приведены в табл. 2.

Таблица 1

Понятие	Определение	Условное обозначение
Раздел	– некоторая выделенная и уникально поименованная часть предметной области	Раздел
Класс объектов	– совокупность типов объектов, объединяющих экземпляры объектов, выделенные по нескольким значительным качественным признакам, и идентифицируемая именем	КлассО
Тип объектов	– совокупность схожих по нескольким значительным качественным признакам экземпляров объектов, идентифицируемая именем	ТипО
Экземпляр объекта	– однозначно идентифицируемый объект из набора объектов, принадлежащих некоторому типу и классу объектов	ЭкзО
Характеристика типа объектов	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих тип объектов определенного класса	ТипХОп
Фактическая характеристика объекта	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих экземпляры объектов определенного класса	ТипХОф
Значение характеристики объекта	– значение, присвоенное характеристике экземпляра объекта	ЗначХО
Класс событий	– совокупность событий (экземпляров событий), выделенных по некоторым качественным признакам, которые могут происходить с экземплярами объектов определенного класса в некоторый момент или интервал времени, и идентифицируемая именем	КлассС
Событие (экземпляр события)	– факт или действие, которое происходит (произошло, будет происходить) с некоторым объектом в определенный момент или интервал времени Идентифицируется временем и объектом, принадлежит некоторому классу событий С одним экземпляром объекта в один и тот же момент (интервал) времени может происходить только одно событие одного класса (при допустимости нескольких событий разных классов)	ЭкзС
Характеристика события	– один поименованный признак (качество, свойство) из всей совокупности признаков, описывающих событие определенного класса	ТипХС
Значение характеристики события	– значение, присвоенное характеристике экземпляра события, которое произошло с конкретным экземпляром объекта	ЗначХС
Класс параметров объектов	– совокупность характеристик параметров объектов, выделенных по некоторым качественным признакам, идентифицируемая именем	КлассПО
Характеристика параметра объекта	– изменяемый во времени один поименованный признак (качество) из всей совокупности признаков, описывающих экземпляры объектов определенного класса	ТипХПО
Единица физической величины	– символьное обозначение единиц физической величины	ЕдИзмер
Документ	– структурированные или неструктурированные данные, необходимые для дополнения, детализации описания существенных свойств (признаков, качеств), связываемых с основными базовыми понятиями модели	Документ
Папка документов	– поименованная совокупность документов, выделенных по каким-либо признакам	Папка

В данной нотации модели «объект-событие», как следует из табл. 2, имеется возможность определения элементов моделируемой ПрО, их характеристик, а также некоторых ограничений целостности.

В состав задаваемых ограничений целостности входят: ограничения на допустимые значения для соответствующих характеристик объектов, событий, параметров объектов, единиц физических величин; ограничения на максимальное количество значений, которые могут быть присвоены определенной характеристике экземпляра события заданного класса; ограничения на максимальное количество экземпляров объектов определенного класса. Кроме того в данной диаграммной нотации возможно явное представление ограничений по существованию, в том числе ссылочной целостности, путем указания связей «владелец-подчиненный» между соответствующими элементами (компонентами) разработанного выразительного средства (языка концептуального моделирования).

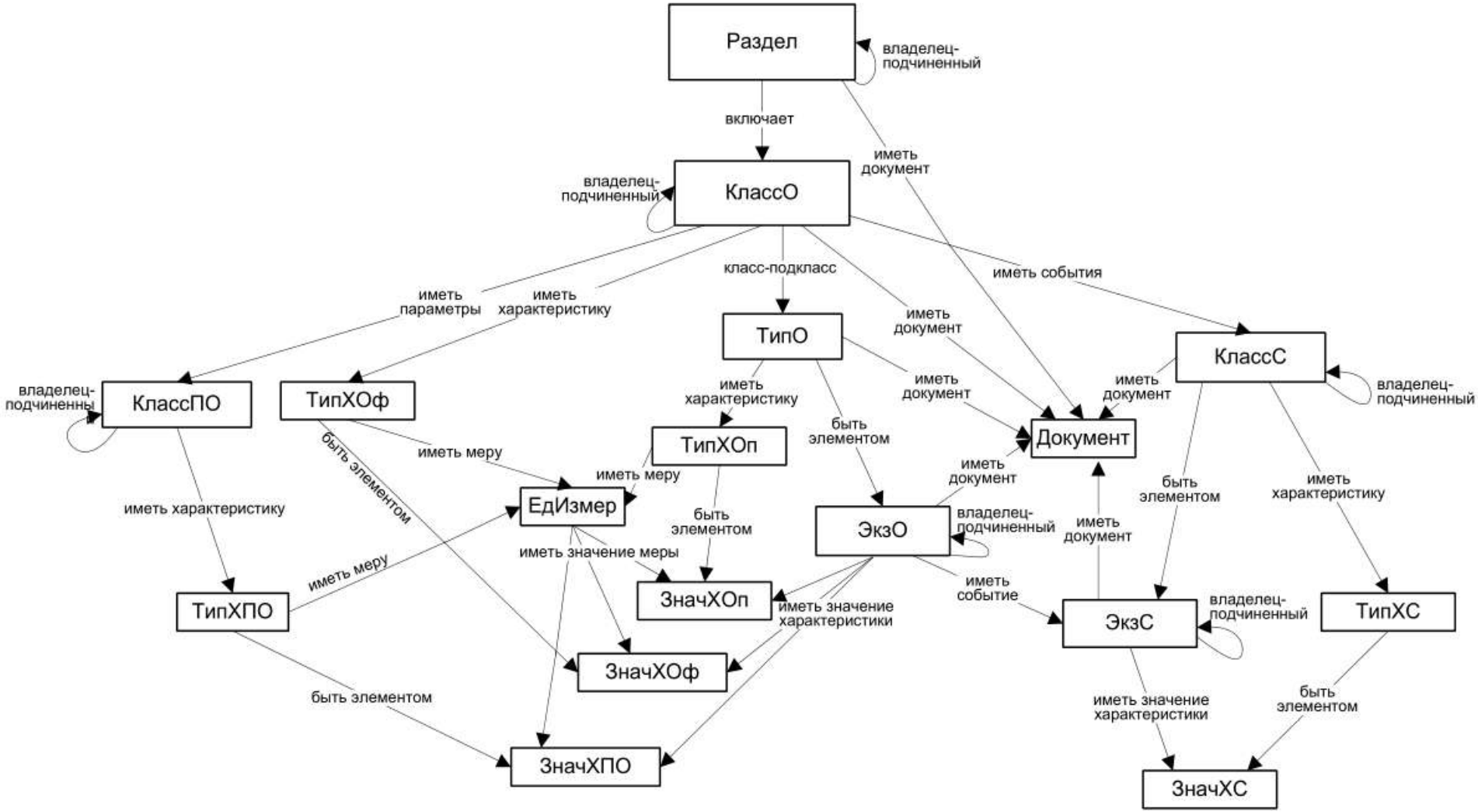
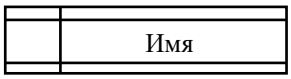
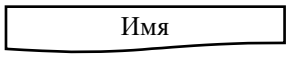
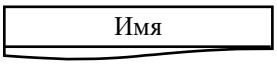


Рис. 1. Представление основных базовых понятий модели данных «объект-событие» и отношений между ними

Таблица 2

Элемент диаграммы	Назначение (описание)
Имя	Определение класса объекта
Имя	Определение «подчиненного» класса объекта
Имя $max_{obj}=M$ fact-char-name1 fact-char-name2 [unit] fact-char-name3: comp-char-name31, comp-char-name32	Определение класса объекта с фактическими характеристиками (fact-char-name1, 2, 3,… – имена характеристик) и ограничениями, накладываемыми на максимальное количество экземпляров объектов этого класса ($max_{obj}=M$, где max_{obj} – ключевое слово, $M \in \mathbb{N}^+$) Имя фактической характеристики объекта, принадлежащей к перечисляемому (списочному) типу, заканчивается символом двоеточия (**:**) и подчеркивается чертой (fact-char-name3:), а допустимые ее значения (comp-char-name31, comp-char-name32, …) следуют под ней с отступом вправо через запятую. При необходимости указания единицы физической величины, в которой измеряются значения характеристики, после имени характеристики в квадратных скобках указывается символьное обозначение единицы (unit), например [км]
Имя	Определение класса событий
Name char-ev-name1 char-ev-name2=N … char-ev-name3: comp-name31, comp-name32 …	Определение класса события с характеристиками (char-ev-name1, 2, 3,… – имена характеристик) и ограничениями, накладываемыми на максимальное количество значений, которые могут быть присвоены указанной характеристике экземпляра события (char-ev-name2= N ; …, $N \in \mathbb{N}^+$) этого класса Имя характеристики события, принадлежащей к перечисляемому (списочному) типу, заканчивается символом двоеточия (**:**) и подчеркивается чертой (char-ev-name3:), а допустимые ее значения (comp-name31, comp-name32, …) следуют под ней с отступом вправо через запятую При необходимости указания единицы физической величины, в которой измеряются значения характеристики, после имени характеристики в квадратных скобках указывается символьное обозначение единицы, аналогично как для характеристики класса объектов
Имя	Определение «подчиненного» класса событий
	Определение связи между базовыми понятиями модели (кроме связи между классами событий) При необходимости (для большей наглядности) могут указываться стрелки, показывающие направление связи
	Определение связи между классами событий При необходимости могут указываться стрелки, показывающие направление связи
Name	Определение типа объекта
Имя pas-char-name1 pas-char-name2 pas-char-name3: comp-pchar-name31, comp-pchar-name32	Определение типа объекта с паспортными характеристиками объекта (pas-char-name1, 2, 3, … – имена характеристик) Имя паспортной характеристики объекта, принадлежащей к перечисляемому (списочному) типу, заканчивается символом двоеточия (**:**) и подчеркивается чертой (pas-char-name3:), а допустимые ее значения (comp-pchar-name31, comp-pchar-name32, …) следуют под ней с отступом вправо через запятую При необходимости указываются единицы физической величины, в которой измеряются значения характеристики (правила их описания аналогичны правилам для характеристик классов объектов и событий)
Имя	Определение класса параметров объектов
Имя	Определение «подчиненного» класса параметров объектов
Имя	Определение раздела предметной области

Продолжение таблицы 2

Элемент диаграммы	Назначение (описание)
	Определение «подчиненного» раздела (подраздела) предметной области
	Определение папки документов
	Определение подпапки документов

Результатом моделирования ПрО, выполненного с помощью предлагаемого выразительного средства, является концептуальная схема ПрО, представленная в виде диаграммы модели «объект-событие», по сути близкой к ER-диаграммам и диаграммам классов языка UML.

Пример представления концептуальной схемы ПрО в виде диаграммы модели «объект-событие» приведен на рис. 2. Концептуальная схема ПрО, представленная в диаграммной нотации модели «объект-событие» – это в первую очередь документированное представление, которое полезно не только при проектировании БД, но и в дальнейшем, при ее эксплуатации, сопровождении и модернизации.

Однако, решая задачу представления концептуальной схемы ПрО, необходимо, как отмечается в работе [8], не только учитывать выразительность средств, благодаря которым такое описание становится достаточно прозрачным для разработчиков и пользователей БД, но и аспекты дальнейшей компьютерной реализации. В том числе, возможности комплексного использования модели, как на этапе проектирования БД (в качестве инструмента концептуального моделирования ПрО), так и на стадии функционирования БД, как основы пользовательских интерфейсов [9]. А это достаточно сложно обеспечить с использованием возможностей разработанного выразительного средства. К тому же с помощью имеющихся типов элементов диаграмм, принципов их формирования и правил организации их взаимосвязей, достаточных для представления метаданных моделируемой ПрО (интенсионала ПрО), невозможно явно представить динамику изменения данных ПрО, что позволило бы расширить возможности по адекватному отображению реального мира и усилило бы контроль за непротиворечивостью данных – ограничением их целостности. Как равным образом невозможно с помощью имеющихся типов элементов диаграмм задать ограничения на множества допустимых экземпляров объектов, являющихся также неотъемлемой и востребованной частью описания ПрО, позволяющих уменьшить количество возможных ошибок впоследствии при реализации. Все это в целом привело к необходимости разработки другого выразительного средства, лишенного указанных недостатков.

Представление концептуальной схемы предметной области в виде ориентированного графа

Значительное влияние на создание предлагаемого ниже выразительного средства представления концептуальной схемы ПрО, как и на создание модели данных «объект-событие» в целом, оказали объектная и семантические сетевые модели. Среди многообразия последних из них особо следует отметить концептуальные графы с принятыми для них ANSI-стандартами, определенными базовыми универсальными примитивами для построения семантических сетей с произвольными отношениями, имеющими возможность включения изображений, аудиоинформации и других концептуальных графов как объектов (вершин графа) [1].

Описательные возможности представления ПрО с помощью графов известны достаточно давно. Граф может использоваться как для представления агрегатов типов сущностей, типов связей, так и их экземпляров [8]. Это все стало побудительным мотивом применения графов для представления концептуальных моделей ПрО.

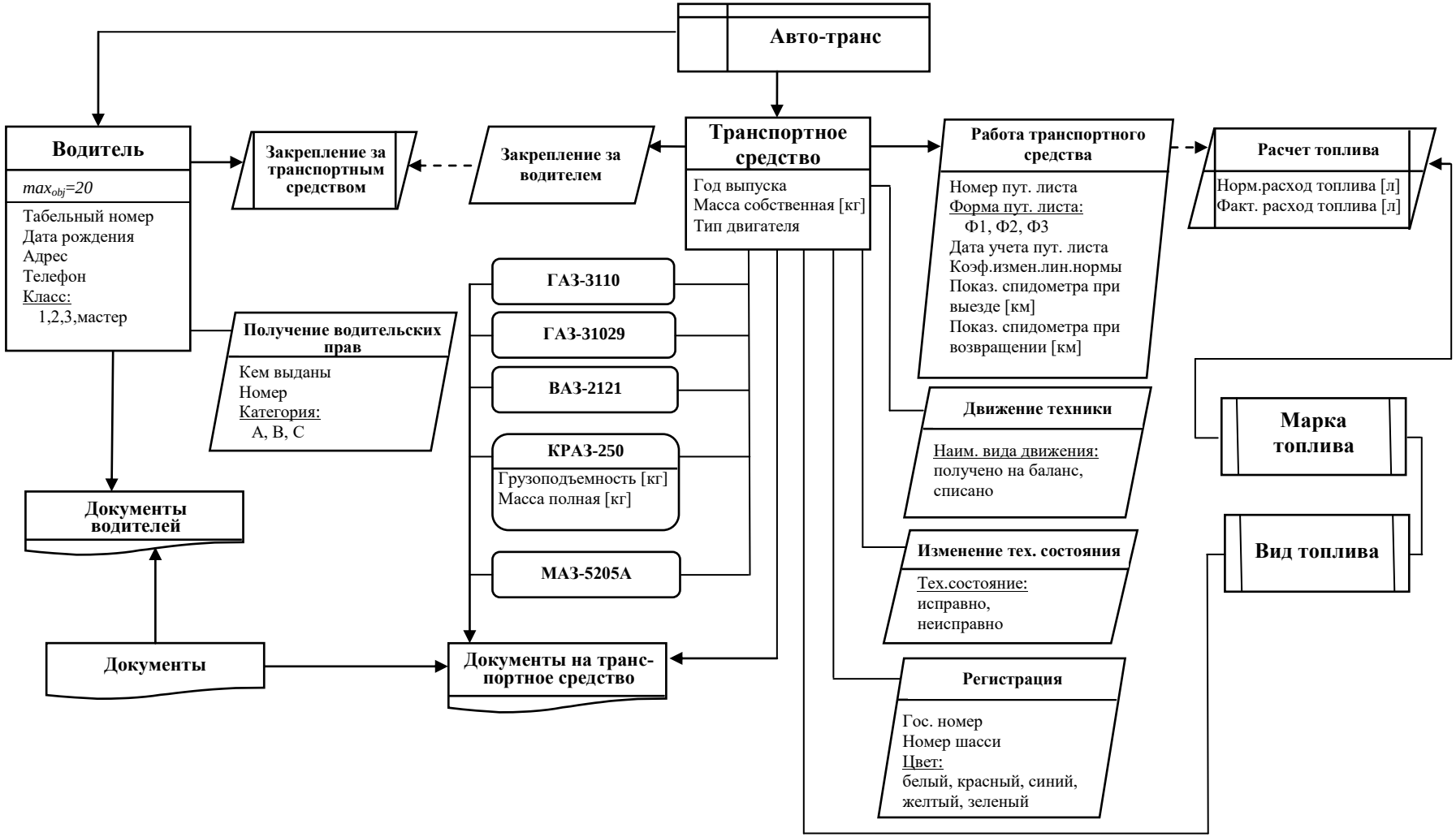


Рис. 2. Пример представления концептуальной схемы ПрО в виде диаграммы модели «объект-событие»

А именно, связных размеченных (помеченных) ориентированных графов $G=(V,E)$, в которых множество $V=V_1\bigcup V_2$ ($V_1\bigcap V_2=\varnothing$) – это множество вершин двух типов: V_1 и V_2; $E=E_1\bigcup E_2$ – множество дуг (ориентированных ребер). Вершины из множества V_1 размечены именами – условными обозначениями основных понятий модели «объект-событие» (таблица 1), вершины из V_2 – именами элементов одноименных соответствующим понятиям множеств. Дуги из множества E_1 соответствуют (помечены) типам взаимодействия между понятиями модели, точнее соотносимых с ними одноименных множеств, и элементами этих множеств. Дуги из множества E_2 соединяют оставшиеся вершины графа и соответствуют таким типам взаимодействия, как «владелец-подчиненный», «иметь событие», «иметь характеристику» и т. д.

Максимальный остовный подграф графа $G=(V,E)$, не содержащий ребер $e_i\in E$ ($i=1...m$) между вершинами $v_j\in V_2$ ($j=1...l$), связывающими классы событий (экземпляры событий) «владельцев» с «подчиненными» классами событий (экземплярами событий), а также связывающими все основные семантические концепции модели (кроме любой одной связи) с понятием «папка документов», является деревом (остовным деревом), которые, как известно, благодаря предельной простоте строения нашли широкое применение в разных областях знания при описании структур различных объектов реального мира [13]. На рис. 3 приведен вариант представления метаданных абстрактной моделируемой ПрО (модель ПрО, отображающая ее свойства, инвариантные во времени, – есть интенсионал ПрО) с помощью связного ориентированного графа $G=(V_1\bigcup V_2,E_1\bigcup E_2)$, в котором для обозначения вершин используются различные геометрические примитивы: прямоугольниками обозначаются вершины из V_1, а четырехугольниками со скругленными углами – вершины из V_2.

При этом имена вершин из множества V_1 – это условные обозначения понятий модели (табл. 1), а ребра E_2 – типы взаимодействия (отношения) между понятиями (ориентированный граф рис. 1). Множество ориентированных ребер из множества E_1, имеют одинаковое имя типа взаимодействия между понятиями модели и элементами их одноименных множеств – «класс-элемент». Имена, которыми размечены вершины из V_2, – произвольные, с индексами, указывающими на возможное существование различного числа соответствующих элементов одноименных множеств, соотнесенных с понятиями модели. Например, $КлО_1$, $КлО_2$,..., $КлО_L$ – имена классов объектов 0-уровня иерархии (без владельцев); $Р_{N1...k_1}$,..., $Р_{N1...k_h}$ – имена разделов (k-1)-уровня иерархии; $Тхс_1$, ..., $Тхс_\eta$ – имена характеристик событий; $ЗнСхоф_1$, ..., $ЗнСхоф_x$ – допустимые значения фактической характеристики объекта, принадлежащей к перечисляемому (списочному) типу и т. д.

Однако приведенный выше в виде графа G вариант представления интенсионала предметной области не в полной мере отражает возможности модели «объект-событие». Как видно из рис. 3, в такой нотации отсутствует возможность задания ограничений целостности. В частности, таких как: ограничения на максимальное количество значений, которые могут быть присвоены определенной характеристике экземпляра события заданного класса; ограничения на максимальное количество экземпляров объектов определенного класса; ограничение на используемые единицы физических величин характеристик объектов, событий, параметров объектов рассматриваемой ПрО. Кроме того, при большом количестве элементов одноименных множеств, соотнесенных с соответствующими базовыми понятиями модели «объект-событие», такое представление становится непростым в восприятии. Сложности возникают и в создании пользовательского интерфейса, обеспечивающего поддержку подобного представления ПрО на стадии функционирования БД.

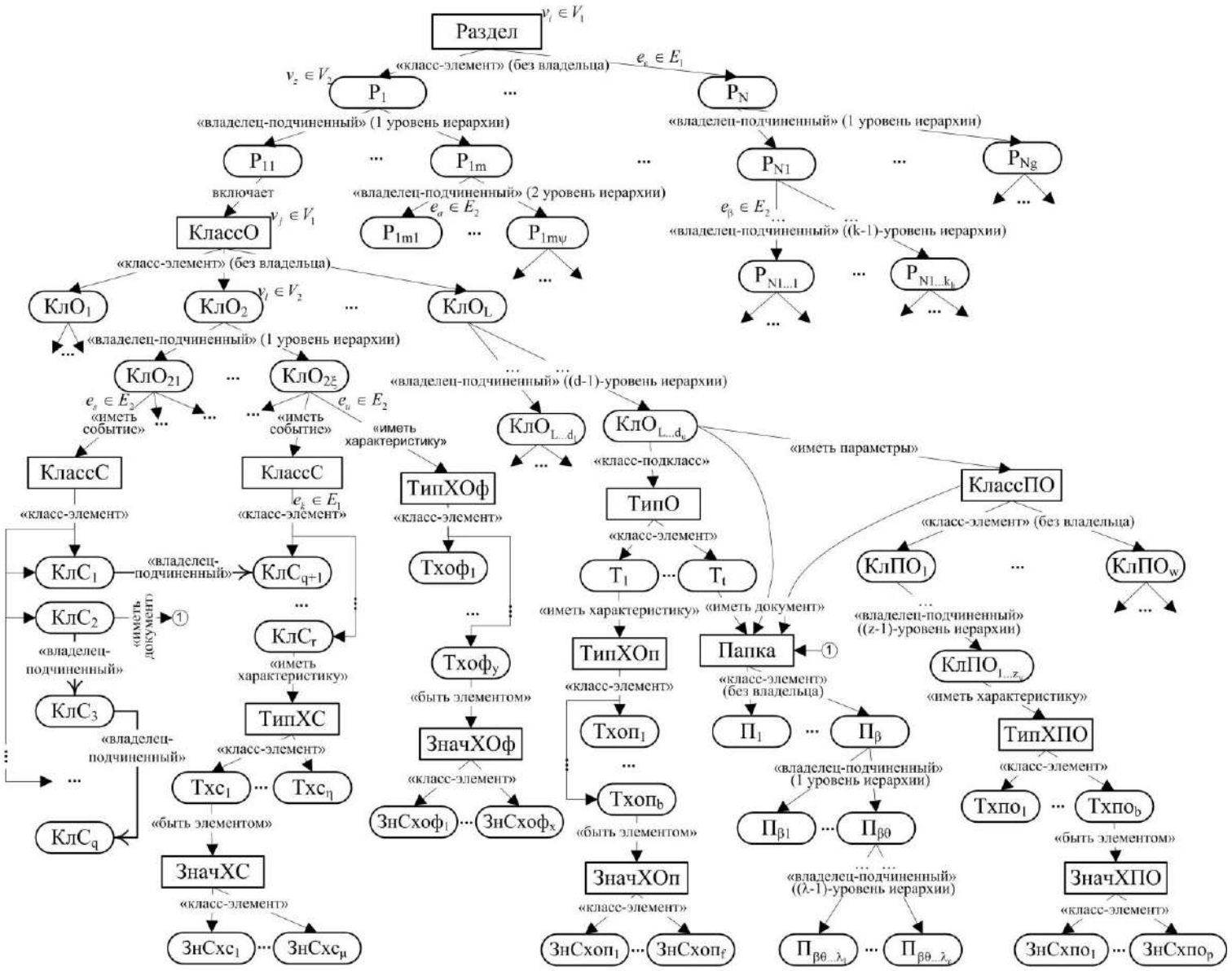


Рис. 3. Представление метаданных ПрО с помощью связного ориентированного графа модели «объект-событие»

Поэтому, опираясь на достоинство приведенного выше представления интенсионала ПрО, и учитывая возможность представления графов в различных формах (о чем отмечается в работах [1, 8], стандарте ISO/IEC 24707:2007), в том числе линейных, для представления концептуальной схемы ПрО предлагается использовать специальную форму записи ациклического ориентированного графа с соответствующими условными обозначениями.

Основные обозначения и задание ограничений целостности (нотация языка). Понятия (полные имена) модели «объект-событие», представляющие собой по аналогии с графом G (рис. 3) его вершины из множества V_1, указываются заключенными в квадратные скобки. Под ними, по направлению стрелок, которые соответствуют ребрам (дугам) E_1 того же графа G, указываются элементы множеств, с которым соотносится каждое понятие, в виде условных обозначений соответствующих понятий, заключенных в угловые скобки, с присвоенными им значениями (именами) после знака равенства (например, <Раздел>=P_1). При этом допускаются комментарии, которые заключаются в кавычки (« »," ") и размещаются, как правило, после определения элементов базовых понятий (в общем случае в любом месте). Для наглядности (удобства восприятия) предлагается делать отступы для соответствующих понятий и располагающихся под ними элементами соответствующих множеств.

Стрелки, ведущие от некоторого элемента множества к определенному понятию, заключенному в квадратные скобки, соответствуют направленным ребрам E_2 с типом взаимодействия между ними аналогично указанному на рис. 3. Стрелки, ведущие от некоторого элемента множества к другому элементу этого же множества (соответствуют направленным ребрам из E_2 с типом взаимодействия «владелец-подчиненный») указывают на иерархию между соответствующими элементами. Определение иерархических имен с помощью такого представления обеспечивает уникальную идентификацию, ссылочную целостность и ограничение по существованию.

Для задания ограничений на максимальное количество экземпляров объектов определенного класса после присвоения имени класса объекта в круглых скобках указывается положительное число $M \in \mathbb{N}^+$. Аналогично для задания ограничений на максимальное количество значений, которые могут быть присвоены определенной характеристике экземпляра события заданного класса, после определения имени характеристики события также в круглых скобках указывается требуемое положительное число.

Чтобы задать ограничения на допустимые значения (определить множество допустимых значений) для соответствующих характеристик объектов, событий, параметров объектов необходимо: ниже введенного уточняющего понятия «списочные значения характеристики» (связанного с некоторым выделенным подмножеством из соответствующих множеств, с которыми соотносятся базовые понятия модели: значение характеристики объекта, события, параметра объекта), по направлению стрелок, которые соответствуют ребрам E_1, через запятую перечислить эти значения. Следующим учитываемым ограничением в предлагаемой нотации, является ограничение, накладываемое на используемые единицы физических величин характеристик объектов, событий, параметров объектов рассматриваемой ПрО. Для задания данного типа ограничений, после присвоенного соответствующей характеристики имени, в фигурных скобках указывается имя физической величины, в которой она измеряется (например, {*unit*}). Фрагмент представления метаданных (интенсионала) моделируемой ПрО в виде объединения нескольких деревьев, образующих ориентированный ациклический граф в соответствующей нотации, эквивалентный фрагменту графа, изображенному на рис. 3, приведен на рис. 4.

Под *метаданными* ПрО (интенсионалом ПрО) в модели «объект-событие» понимается совокупность конкретных разделов; классов: объектов, событий, параметров объектов; типов объектов; характеристик: экземпляров, типов, параметров объектов, событий; доменов допустимых значений соответствующих характеристик: объектов, событий, параметров объектов,

принадлежащих к перечисляемому типу; единиц физических величин; папок документов, как элементов множеств, соотносимых с соответствующими базовыми понятиями модели, с помощью которых отображаются инвариантные во времени свойства (характеристики) моделируемой ПрО. Под *данными* ПрО (экстенсионалом ПрО) в модели «объект-событие» понимается совокупность экземпляров: объектов, событий; значений характеристик: экземпляров объектов, событий, параметров объектов; документов, как элементов множеств, соотносимых с соответствующими базовыми понятиями модели, с помощью которых отображается состояние моделируемой ПрО в зависимости от времени.

Пример эквивалентного представления концептуальной схемы ПрО, выполненного с помощью диаграмм модели «объект-событие» (рис. 2), в рассматриваемой нотации, будет иметь вид, приведенный на рис. 5.

Приведенная выше нотация позволяет представлять не только интенсионал рассматриваемой ПрО, но и ее экстенсионал (все указанные выше правила остаются неизменными, добавляются только некоторые обозначения, связанные с потребностью представления данных ПрО). Это позволяет в дополнение к существующим возможностям, во-первых, визуализировать представление динамики изменения данных ПрО, тем самым усиливая контроль за непротиворечивостью данных (ограничением их целостности) и расширяя возможности по адекватному отображению реального мира; во-вторых, задавать ограничения на множество допустимых экземпляров объектов, позволяющих уменьшить количество возможных ошибок впоследствии при реализации, а, в-третьих, способствует комплексному применению модели (как на этапе проектирования БД, так и на стадии функционирования БД), ввиду возможности определения данных ПрО, необходимых на этапе функционирования БД.

На рис. 6 представлен экстенсионал некоторой моделируемой ПрО в виде специальной нотации графа модели «объект-событие».

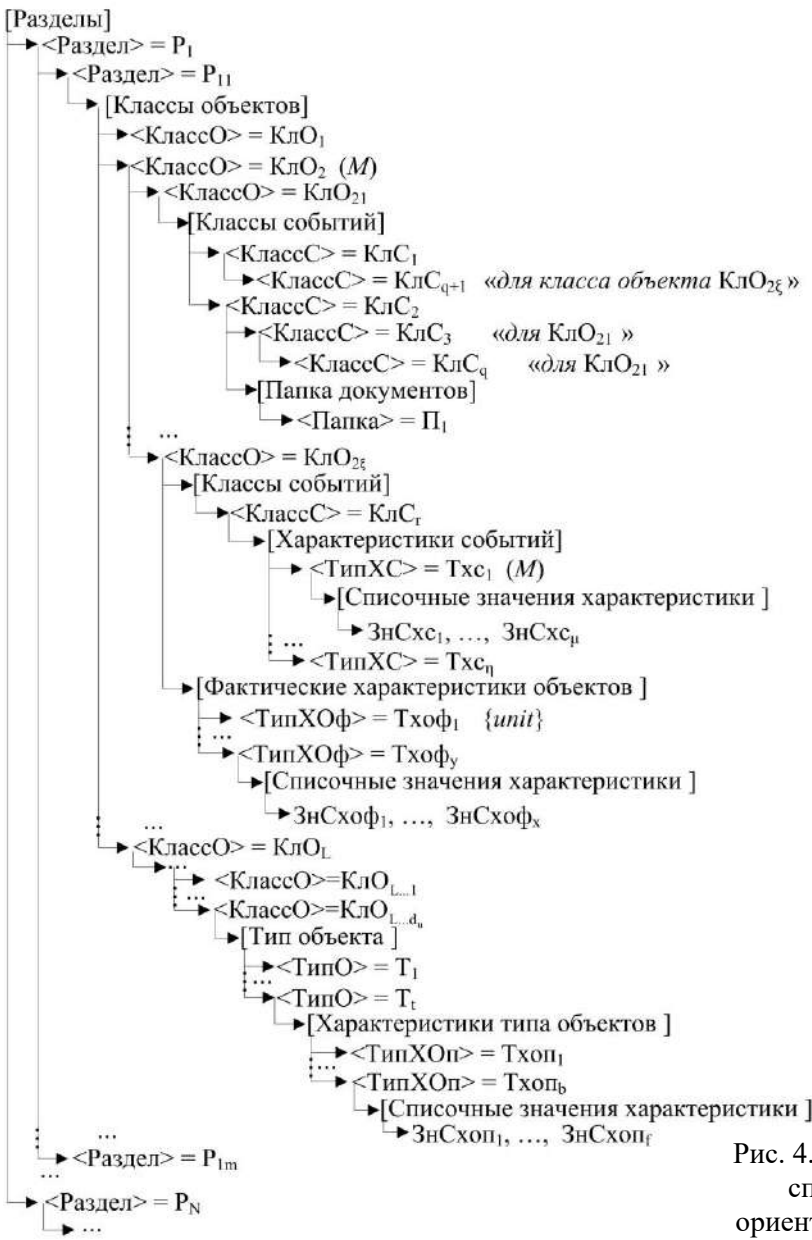


Рис. 4. Представление метаданных ПрО с помощью специальной формы записи ациклического ориентированного графа модели «объект-событие»

Рис. 5. Пример представления интенсионала моделируемой ПрО

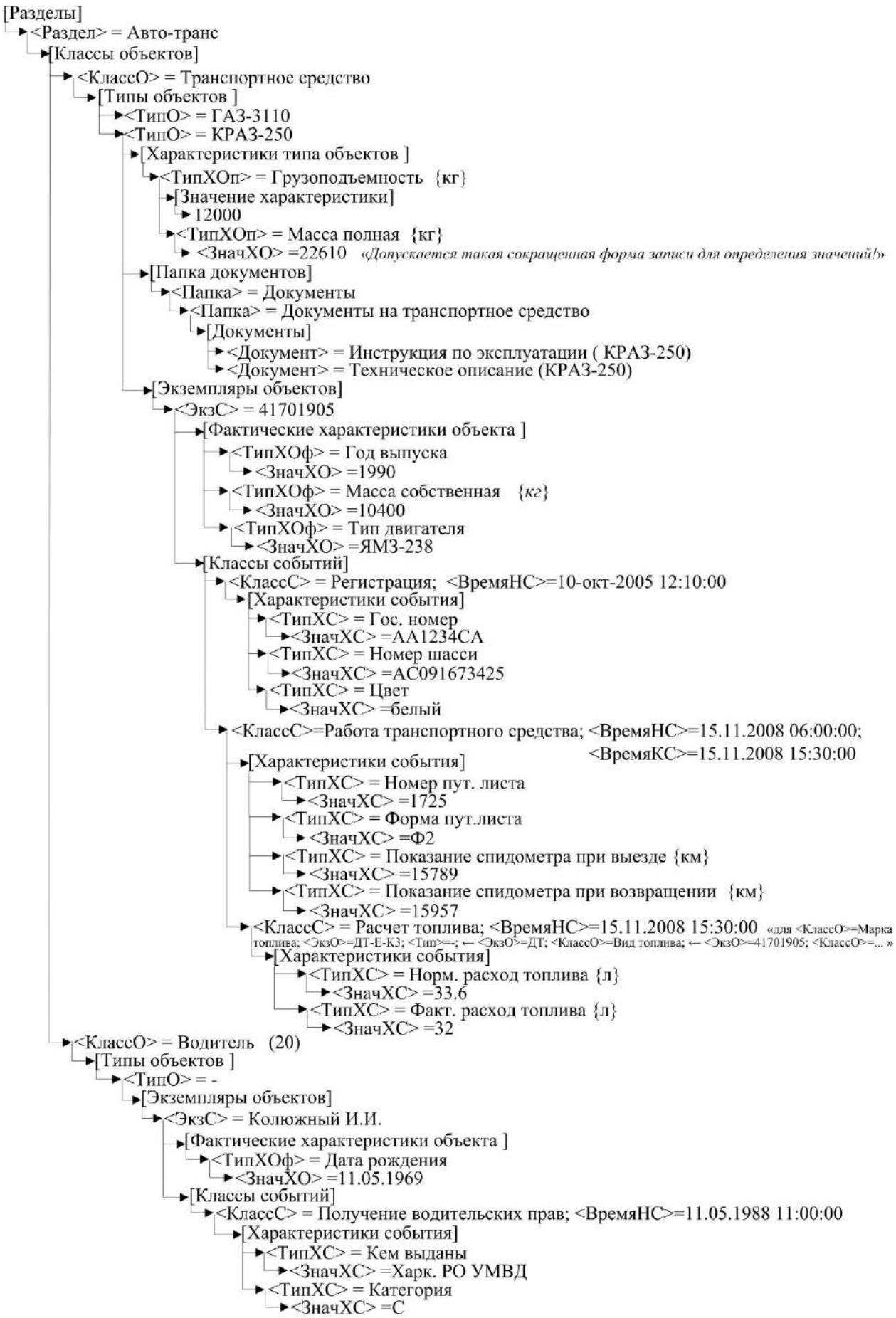


Рис. 6. Пример представления экстенсионала моделируемой ПрО

Комплексное представление ПрО (ее интенсионала и экстенсионала), выполненное с помощью предлагаемого выразительного средства, позволяет прозрачно для участников проекта визуализировать адекватное описание статических и временны*х* свойств объектов моделируемой ПрО вместе со свойственными ей ограничениями. Это свидетельствует о целесообразности применения данной нотации модели «объект-событие» на этапе проектирования БД (в качестве инструмента концептуального моделирования ПрО). С другой стороны, применение предлагаемых связных ориентированных ациклических графов для описания ПрО, совместно с разработанным языком модели данных (ЯМД) [14, 15], близким к некоторому подмножеству естественного языка, способствующим решению задачи автоматической трансформации семантически правильных запросов, составленных в терминах ПрО, в синтаксически и терминологически корректные запросы к конкретной БД (то есть, как основы пользовательских интерфейсов), являющимся в определенной степени результатом отображения формы представления данных ПрО в виде графов в линейную, позволило реализовать возможность комплексного использования модели данных «объект-событие», как на этапе концептуального проектирования БД, так и на стадии функционирования реляционных баз данных.

Выводы

1. В результате анализа существующих достижений в области семантического моделирования и перспективных направлений ее развития, исходя из необходимости нахождения новых решений проблемы, связанной с потребностью своевременного создания, модернизации в рамках запланированного бюджета баз данных, обладающих требуемыми качествами, для представления концептуальных схем ПрО были разработаны выразительные средства, как системы определенных графических обозначений (знаков), включающие ограниченное число различных элементов, представляющих основные понятия модели «объект-событие» и связи между ними в виде определенных геометрических фигур или линейной формы представления с правилами их описания. А именно, выразительные средства представления концептуальных схем различных ПрО в виде диаграммы модели данных «объект-событие» и в виде ациклического ориентированного графа.

2. Выразительное средство представления концептуальных схем различных ПрО в виде диаграммы модели данных «объект-событие» позволяет графически представлять интенсионал моделируемой предметной области в терминах базовых понятий модели, элементы соотносимых одноименных множеств которых ассоциируются с метаданные ПрО, и отношений между ними. Это в первую очередь средство документированного представления концептуальной схемы предметной области, коммуникационного посредника в информационном обмене между аналитиками, разработчиками, специалистами ПрО, программистами и пользователями, полезного как при проектировании БД, так и в дальнейшем, при их эксплуатации, сопровождении и модернизации.

3. С целью выполнения предъявляемых к модели требований, средства которой также должны обеспечивать возможность комплексного ее использования, как на этапе концептуального проектирования, так и на стадии функционирования БД, было разработано новое выразительное средство, так как средство представления ПрО в виде диаграмм модели данных «объект-событие» не в полной мере удовлетворяло этому требованию. Предлагаемая нотация этого средства, позволяющая представлять в виде объединения нескольких деревьев не только интенсионал рассматриваемой ПрО, но и ее экстенсионал, обеспечивает возможность адекватного представления структур, статических и временных свойств объектов моделируемой ПрО вместе со свойственными ей ограничениями. Такое комплексное представление способствует применению модели, как на этапе концептуального проектирования реляционной БД, так и на стадии ее функционирования.

4. Совместное применение разработанных выразительных средств представления данных моделируемых предметных областей: специальной нотации ациклического ориентиро-

ванного графа и языка модели данных, позволяет реализовать возможность комплексного использования модели данных «объект-событие», как на этапе концептуального проектирования БД (в качестве инструмента концептуального моделирования ПрО), так и на стадии функционирования реляционной БД (как основы пользовательских интерфейсов).

Список литературы: 1. *Палагин А. В.* Онтологические методы и средства обработки предметных знаний: монография / А. В. Палагин, С. Л. Крывый, Н. Г. Петренко. – Луганск : изд-во ВНУ им. В. Даля, 2012. – 323 с. 2. *Сорока Л. С.* Формализованное представление модели данных «объект-событие» / Л. С. Сорока, В. И. Есин // Вісник Академії митної служби України. Сер.: Технічні науки. – 2011. – № 2(46). – С. 49–62. 3. *Есин В. И.* Модель данных «объект-событие» и ее возможности / В. И. Есин, В. Г. Юрасов // Вестник Воронежского государственного технического университета. – 2014. – Т. 10, № 4. – С. 38-43. 4. *Есин В. И.* Универсальная модель данных и ее математические основы / В. И. Есин // Системи обробки інформації. – 2011. – № 2(92). – С.21-24. 5. *Есин В. И.* Универсальная модель данных и ее отличительные особенности / В. И. Есин // Вісник Харківського національного університету імені В. Н. Каразіна. Сер.: Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. – 2011. – № 960. – С. 141-147. 6. *Есин В. И.* Модель данных с универсальной фиксированной структурой / В. И. Есин // Теоретичні та прикладні аспекти побудови програмних систем : матеріали міжнародної наукової конференції, м. Київ, 15-17 грудня 2014 р. – Кіровоград : ФО-П Александрова М. В., 2014. – С. 112-116. 7. *Date C. J.* An Introduction to Database Systems, 8th Edition / C. J. Date. – Pearson. Addison-Wesley, 2004. – XXVII, 983, I-22 p. 8. *Цикритзис Д.* Модели данных / Д. Цикритзис, Ф. Лоховски ; пер. с англ. – М. : Финансы и статистика, 1985. – 344 с. 9. *Когаловский М. Р.* Системы доступа к данным, основанные на онтологиях / М. Р. Когаловский // Программирование. – 2012. – № 4. – С. 55-77. 10. *Когаловский М. Р.* Концептуальное моделирование в технологиях баз данных и онтологические модели / М. Р. Когаловский, Л. А. Калиниченко // Тр. Симпозиума «Онтологическое моделирование». – М. : ИПИ РАН, 2008, С. 114-148. 11. *Гарсиа-Молина Г.* Системы баз данных // Г. Гарсиа-Молина, Д. Д. Ульман, Д. Уидом. – М. : Изд. дом "Вильямс", 2003. – 1088 с. 12. *Цаленко М. Ш.* Моделирование семантики в базах данных / М. Ш. Цаленко. – М. : Наука. Гл. ред. физ-мат. лит., 1989. – 288 с. 13. *Харари Ф.* Теория графов / Ф. Харари. – М. : Мир, 1973. – 300 с. 14. *Есин В. И.* Язык для универсальной модели данных / В. И. Есин, М. В. Есина // Системи обробки інформації. – 2011. – № 5(95). – С.193-197. 15. *Есин В. И.* Язык описания и манипулирования данными, хранящимися в БД с УМД / В. И. Есин, М. В. Есина // Компьютерное моделирование в наукоемких технологиях (КМНТ-2010) : междунар. науч.-техн. конф., 18-21 мая 2010 г. : тезисы докл. – Х. : ХНУ им. В.Н. Каразина, 2010. – Ч. 2. – С. 104-108.

Харьковский национальный
университет имени В.Н.Каразина

Поступила в редколлегию 05.10.2017

УДК 638.235.231

В.А. ГОРБАЧЕВ, канд. техн. наук, проф., К.Б. АБДУЛРАХМАН

ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ

1. Введение. Актуальность

До некоторого времени безопасность компьютерной системы традиционно связывали с безопасностью программного обеспечения или обрабатываемой информации. Аппаратные ресурсы, используемые для обработки информации, считались надежными. Появление аппаратных закладок (АЗ), в зарубежной литературе известных как Hardware Trojan (HT), и угроз, связанных с ними, нарушило это доверие. АЗ могут быть реализованы в ASIC и в FPGA, в имеющихся на рынке микропроцессорах, микроконтроллерах, сетевых процессорах или цифровых процессорах сигналов (DSP). Таким образом, требование безопасности электронных систем – это такое же ограничение, как низкая потребляемая мощность, высокая скорость, устойчивость к отказам и т.д.

Приведем несколько важных характеристик АЗ:

1. Сложность ИС и чрезвычайно малые размеры АЗ делают практически невозможным ее обнаружение без специальных инструментальных средств.

2. Даже в случаях, когда факт нарушения безопасности будет выявлен, доказать, что это действие выполнено АЗ, очень сложно.

3. АЗ обладают свойством перманентности: как только в систему была встроена АЗ, угроза сохраняется всегда, когда система находится во включенном состоянии.

4. АЗ расположены ниже программного блока, включающего операционную систему, программное обеспечение (middleware), работающее поверх операционной системы, и приложения. Это позволяет АЗ или полностью обойти традиционные программные средства защиты информации, или сделать их малоэффективными.

Эти и другие характеристики делают такие закладные устройства очень перспективным элементом при планировании электронных диверсий.

2. Классификация АЗ

Разработка эффективных методов, предназначенных для обнаружения и блокировки АЗ зависит от полноты характеристик АЗ и схемы классификации.

Классификация АЗ – это дерево, где каждая ветвь определяет другую характеристику (или атрибут) АЗ. В идеальном случае определенная АЗ должна находиться только на одном листе дерева.

Классификация АЗ позволяет определить значимость каждой из характеристик АЗ, ее влияние на систему, а также выявить этапы разработки системы, на которых АЗ могут быть устранены. Кроме того, классификация АЗ имеет и самостоятельное значение – ее можно использовать как основу для анализа и разработки методов обнаружения и предупреждения АЗ данных классов. Более того, классификация АЗ позволяет осуществить экспериментальное тестирование систем защиты, т.к. она позволяет выбрать направления и способы проведения тестовых атак на наиболее уязвимые компоненты систем защиты.

Существует несколько методов классификации АЗ. Эти методы используют различные характеристики АЗ. Наиболее распространенными являются следующие характеристики АЗ: физические свойства, механизм активации и функциональное действие.

Например, в [1, 2] АЗ классифицируются по трем признакам: физическим свойствам, механизмам активации и функциональному воздействию. Подробная классификация АЗ, где рассмотрены многие характеристики, рассмотрена в [3, 4] и представлена на рис. 1.

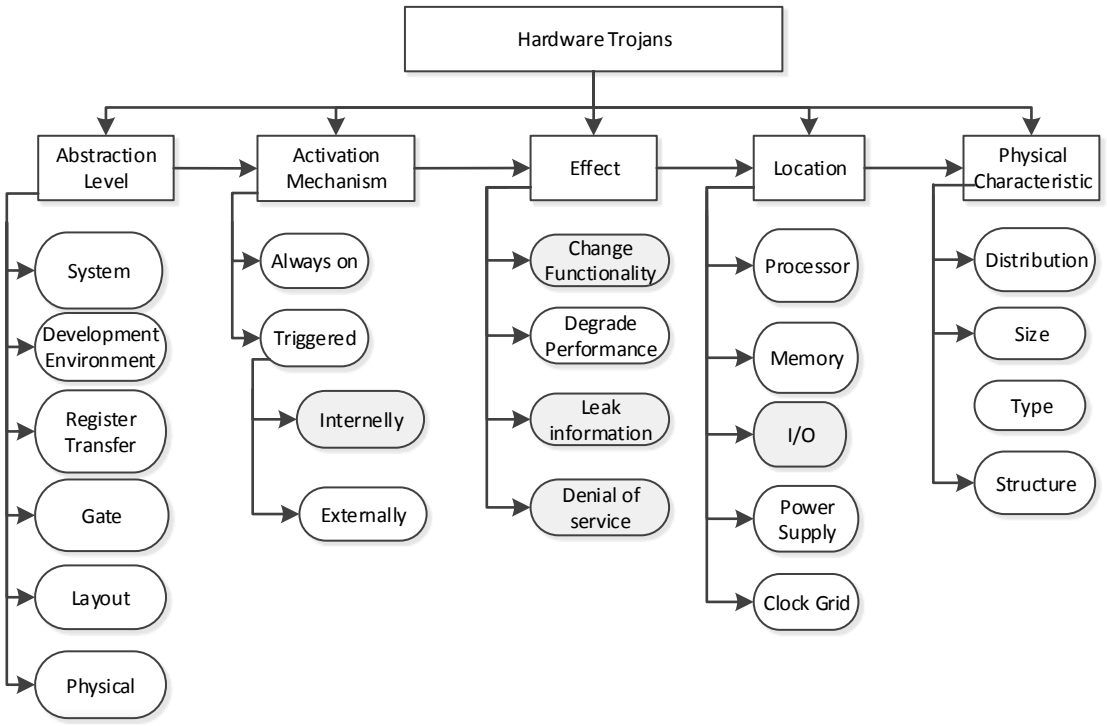


Рис. 1

Учитывая то, что угрозы АЗ направлены на нарушение безопасности информации, в работе [5] предлагается следующая классификация АЗ по их функциональному воздействию (Effect): нарушающие конфиденциальность, целостность и доступность информации.

Важно отметить, что сложность АЗ изменялась от простых, встроенных, например, в клавиатуру [6], до сложных, встроенных, например, в процессор [7].

В результате анализа литературных источников по классификации АЗ сделаем следующие выводы:

1. Множество угроз постоянно расширяется и имеет тенденцию экспоненциального роста. Это означает, что невозможно создать исчерпывающую классификацию АЗ [4].

2. Пространство проектных решений АЗ слабо изучено. Ошибочно утверждать, что целью АЗ является атака на аппаратные ресурсы системы. Возможность атаки АЗ на программный стек, лежащий выше аппаратных ресурсов, является реальной.

3. Электронные системы могут быть заражены одновременно несколькими АЗ, которые могут совместно разрушить систему защиты.

4. Структура АЗ может быть распределенной, что значительно увеличивает сложность ее обнаружения.

3. Методы борьбы с АЗ

Существуют два основных способа [8], обеспечивающих гарантии того, что, используемая ИС является аутентичной, другими словами, она выполняет только те функции, которые были определены первоначально, и не более того. Первый способ – сделать весь процесс разработки ИС надежным. Этот способ чрезмерно дорогостоящий и практически невозможный, с учетом текущих тенденций в глобальном распределении процессов проектирования и изготовления ИС. Второй способ – проверить аутентичность уже готовых ИС перед их использованием.

Рассмотрим классификацию методов борьбы с АЗ, представленную на рис. 2 [4]. Эти методы можно разделить на два класса: методы обнаружения АЗ и методы предотвращения внедрения АЗ.

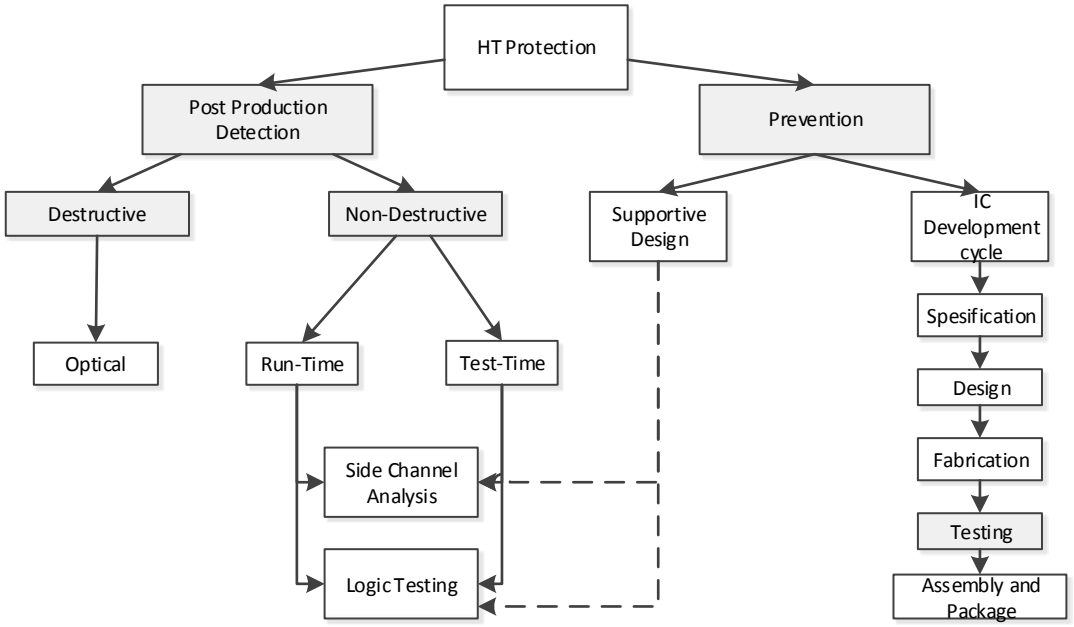


Рис. 2

3.1. Методы обнаружения угроз АЗ

Известно, что невозможно полностью предотвратить внедрение АЗ в ИС на этапе ее производства [8]. В тех случаях, когда превентивные меры, использующиеся для защиты от АЗ, не приносят результата, используются методы обнаружения АЗ, внедренных в структуру ИС. Методы обнаружения АЗ применяются после производства ИС. Существует множество различных методов обнаружения АЗ. Кратко рассмотрим классификацию этих методов (рис. 2), приведенную в [2, 4]. Методы обнаружения АЗ можно представить в виде двух классов: методы, разрушающие и неразрушающие ИС.

Методы, разрушающие ИС. Применяются для определения полной электрической и функциональной схемы. В основе метода лежит химическая полировка металлов, а затем использование сканирующего электронного микроскопа. Полностью уничтожает исследуемую ИС. Характеризуется высокой трудоемкостью и большими материальными затратами.

Методы, не разрушающие ИС. Неразрушающие методы обнаружения АЗ не разрушают ИС и классифицируются как методы, которые обнаруживают АЗ либо во время функционирования (Run-Time), либо во время логического тестирования (Test-Time) интегральной схемы.

Run-Time методы [13] *обнаружения АЗ.* В настоящее время существует большое разнообразие методов обнаружения АЗ, которые осуществляют непрерывный мониторинг характеристик ИС в реальном времени.

Например, авторы [9] подробно описывает метод обнаружения двух типов атак на память ИС: DoS-атака и атака, при которой АЗ отключает защиту памяти. Для обнаружения и блокировки атак предлагается использовать дополнительный защитный модуль, осуществляющий контроль операций обращения к памяти. Этот метод требует, чтобы операционная система была изменена с учетом взаимодействия с защитным модулем.

В [10] для мониторинга безопасности функционирования ИС в режиме реального времени авторы добавили реконфигурируемую логику DEsign-For-ENabling-SEcurity (DEFENSE). После изготовления микросхемы реконфигурируемая логика программируется, подробно описывая поведение ИС. Отклонения в поведении ИС могут быть обнаружены в процессе ее функционирования.

Авторы [11] предлагают обнаруживать АЗ, выполняя функционально эквивалентные процессы на нескольких аппаратных компонентах обработки информации. Затем результаты можно сравнить, выявляя процессы, на которые повлияла АЗ.

В результате анализа методов обнаружения АЗ, осуществляющих непрерывный мониторинг характеристик ИС в реальном времени, приходим к следующим выводам. Run-Time методы обнаружения АЗ:

1. Способны обнаружить только определенный тип АЗ.

2. Являются эффективными при условии, что АЗ находится в активном состоянии.

3. Позволяют осуществлять мониторинг характеристик ИС в реальном времени в критических режимах, в режиме ожидания, а также оценивать политику безопасности, производительность и доступность модулей системы.

Test-Time методы обнаружения АЗ. Test-Time методы обнаружения АЗ, в свою очередь, делятся на два класса: методы логического тестирования и методы, использующие анализ побочных каналов.

Методы логического тестирования (Logic Testing). Много работ посвящено развитию методов логического тестирования**.** Достаточно подробный анализ работ, посвященных данному подходу, можно найти в [2, 3, 6, 12, 13]. Авторы этих работ утверждают, что огромное логическое пространство состояний современной ИС делает невозможным, с вычислительной точки зрения, построение тестового вектора, покрывающего все логическое пространство ИС.

В результате анализа методов логического тестирования, приходим к выводам:

1. Тесты, используемые для обнаружения производственных ошибок, например таких как константная неисправность и задержки, не могут гарантировать обнаружение АЗ. Такие тесты работают со списком соединений ИС, свободной от АЗ, и поэтому не могут активировать и обнаруживать АЗ.

2. Методы логического тестирования не могут обнаружить АЗ, которые не производят воздействия на функциональный выход ИС.

3. Очень проблематично построить исчерпывающий тестовый вектор, обнаруживающий спусковые механизмы АЗ, срабатывающие от времени, например, такие, как time-bombs.

4. АЗ могут находиться в плохо контролируемых и доступных модулях, что делает маловероятным их активацию и обнаружение с использованием случайных или функциональных векторов.

Методы, использующие анализ побочных каналов (Side-Channel Analysis).

Метод анализа побочных каналов [13] использует тот факт, что сам механизм запуска и функционирование АЗ меняет определенные параметры ИС. К параметрам, свидетельствующим о наличии в структуре системы АЗ, относятся: изменение потребляемой мощности, задержки, токи утечки, повышение температуры определенной части ИС.

В [13] рассматривается факт изменения потребляемой мощности как параметр метода для обнаружения АЗ. Проведенные экспериментальные испытания подтвердили эффективность используемого анализа побочных каналов.

Авторы [14] демонстрируют эффективное использование метода побочных каналов, осуществляя сравнение энергопотребления между цепями, инфицированными АЗ, и теми, которые свободны от АЗ. Большие изменения в потреблении мощности могут свидетельствовать о постороннем оборудовании.

В работе [15], в качестве параметра метода анализа побочных каналов, используются задержки, вызванные цепями АЗ.

В результате анализа методов, *использующих анализ побочных каналов*, приходим к следующим выводам:

1. Требуется наличие подлинной, т.е. свободной от АЗ, ИС, которая должна использоваться для сравнения с тестируемой. В то же время, нет никакой гарантии, что оставшиеся ИС свободны от АЗ.

2. Учитывая большое количество IP-модулей, используемых в ИС, а также высокую сложность современных IP-модулей, выявление небольших вредоносных изменений является чрезвычайно сложным.

3. АЗ могут находиться в плохо контролируемых и доступных модулях

4. Совершенствование технологий литографии приводит к тому, что изменения, обусловленные АЗ, все меньше влияют на электрические параметров ИС. Таким образом, обнаружение АЗ с использованием простого анализа параметров сигналов будет неэффективным.

3.2. Методы предотвращения внедрения АЗ

В отличие от методов обнаружения, методы предотвращения угроз АЗ объединяют методы, которые препятствуют внедрению АЗ. Одним из способов гарантирования, что в ИС не будет внедрена АЗ, является жесткое управление жизненным циклом разработки ИС (IC development cycle) на всех его этапах (рис. 2). Это важное звено в стратегии эффективной защиты. Этапами жизненного цикла разработки ИС являются этапы: составления спецификации (Specification), проектирования (Design), изготовления (Fabrication), тестирования (Testing) и сборки (Assembly and Package). Авторы [2] утверждают, что только этапы спецификации и тестирования могут быть не уязвимыми внедрением АЗ. Все другие этапы на практике уязвимы из-за зависимости от сторонних поставщиков IP модулей, от инструментов проектирования и от процесса проектирования и производства.

На этапе проектирования АЗ могут быть внедрены кем-то из разработчиков, или включением в проект инфицированных IP модулей. Различные рекомендации, предотвращающие внедрение АЗ при разработке ИС, рассматриваются в [2, 8, 16].

Особую группу составляют методы (*Supportive design*), которые на этапе проектирования ИС встраивают дополнительные защитные механизмы, блокирующие функционирование предполагаемой АЗ. Эти механизмы могут повышать эффективность методов логического тестирования (Logic Testing) и методов, которые используют анализ побочных каналов (Side-Channel Analysis).

Так, в [17] авторы рассматривают различные защитные механизмы и их практическую реализацию, которые управляют доступом и использованием данных в системе. Эти механизмы блокируют функционирование АЗ определенного типа.

Различные решения по встраиваемым дополнительным защитным механизмам, которые блокируют функционирование определенного типа АЗ, можно найти в [18, 19].

В результате анализа методов предотвращения угроз, приходим к выводу:

- эти методы характеризуются высокими накладными затратами;
- ориентированы на определенные типы АЗ;
- очень сложно полностью предотвратить внедрение АЗ в ИС на этапе ее производства.

4. Выводы. Перспективные направления исследований

Подведем некоторые итоги и сформулируем направление будущих исследований .

Во-первых, современные методы обнаружения, а также методы предотвращения внедрения АЗ не могут обеспечить полную гарантию того, что ИС или электронная система свободны от АЗ.

Во-вторых, рассматриваемые методы способны обнаруживать только определенный тип АЗ.

В-третьих, средства осуществления угроз безопасности (АЗ) выбираются не случайным образом. Новая эффективная АЗ непременно использует определенные особенности архитектуры и функционирования или недостатки средств защиты электронной системы.

В-четвертых, противостояние АЗ и средств защиты напоминает систему с обратной связью – новые типы АЗ приводят к появлению новых средств защиты, а недостатки в средствах защиты приводят к появлению новых типов АЗ и т.д. Разорвать эту обратную связь бесконечного противостояния можно двумя путями:

- создать эффективные и безупречно надежные средства защиты от каждого типа АЗ, или

- устранить причины указанных недостатков электронных систем, которые служат источником успешной реализации угроз безопасности.

Рассмотрим недостатки и преимущества того и другого метода.

Создание средств защиты от каждого вида угроз. К преимуществам данного метода следует отнести то, что средства защиты не зависят напрямую от назначения электронной системы и не требуют модификации по мере ее развития. Недостатки такого подхода очевидны: для создания эффективного механизма защиты необходимо проанализировать все типы АЗ и разработать для каждого типа соответствующий механизм противодействия. Практика показывает, что данный путь трудно осуществим вследствие следующих факторов:

- множество АЗ постоянно расширяется и имеет тенденцию экспоненциального роста. Это означает, что все время будут появляться новые АЗ, требующие новых мер защиты, т. к. старые против них бессильны;

- множество АЗ растет не только количественно, но и качественно, т. к. для того, чтобы АЗ состоялась, она должна принципиально отличаться от тех, на которые рассчитаны системы защиты. Это означает, что невозможно создать исчерпывающую классификацию угроз безопасности и предсказать появление новых типов АЗ.

Устранение причин, обуславливающих успешную реализацию угроз. Этот подход основан на проектировании защищенных систем обработки информации, устраняет причины появления изъянов защиты. Он должен удовлетворять следующим требованиям:

1. Интеграция средств защиты информации, в качестве обязательного элемента, в процесс ее обработки.

2. Включение в модель безопасности (или в механизмы защиты) функций, обеспечивающих безопасность электронной системы в условиях возможного появления внутри ее компонентов, осуществляющих деструктивные действия.

3. Используемые методы проектирования должны основываться на формальных принципах, доказательно обеспечивающих гарантии защищенности систем.

Преимущества этого подхода очевидны: он не зависит от развития АЗ, так как ликвидирует причину, а не следствие, поэтому он более эффективен, чем создание средств защиты от каждого вида АЗ. В качестве недостатков данного подхода можно отметить необходимость применения новых технологий и формальных методов проектирования защищенных электронных систем.

Целью последующего исследования являются *технологии проектирования защищенных ЭС,* обеспечивающие устойчивость ЭС к деструктивному воздействию внутренних компонентов.

Список литературы: 1. *Tehranipoor, M. and Koushanfar, F.* A Survey of Hardware Trojan Taxonomy and Detection // IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10-25, Jan. 2010. 2. *Chakraborty, R. S., Narasimhan, S. and Bhunia, S.* Hardware Trojan: Threats and emerging solutions // IEEE International High Level Design Validation and Test Workshop. IEEE, Nov. 2009, pp. 166-171. 3. *He Li, Qiang Liu, Jiliang Zhang* Survey of hardware Trojan threat and defense // INTEGRATION, the VLSI journal 55, 2016, pp. 426–437. 4. *Julien Francq, Hardware Trojans* Detection Methods, Cassidian Cybersecurity // All rights reserved, in TRUDEVICE, 2013, Page 36 – 40. 5. *Gorbachov, V.* Malicious Hardware: characteristics, classification and formal models // IEEE East-West Design & Test Symposium (EWDTS2014), Kiev, Ukraine, 2014, pp. 254-257. 6. *Горбачев В.А., Степаненко, В.В.* Сертификация периферийных устройств компьютерных систем // Радиотехника. – 2003. – Вып. 134.- С. 206-209. 7. *Samuel, T. King and all* Designing and implementing malicious hardware // LEET'08 Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats Article No. 5 San Francisco, California – April 15 – 15, 2008. 8. *Mark Beaumont, Bradley Hopkins and Tristan Newby*. Hardware Trojans – Prevention, Detection, Countermeasures (A literature Review). DSTO Defence Science and Technology Organisation Edinburgh, South Australia 5111, Australia 2011]. 9. *Bloom, G., Narahari B. & Simha, R.* (2009) OS support for detecting trojan circuit attacks, in IEEE International Symposium on Hardware-Oriented Security and Trust. 10. *Abramovici, M. & Bradley, P.* (2009) Integrated circuit security: new threats and solutions, in Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, CSIIRW '09, ACM, New York, NY, USA, pp. 55:1–55:3. 11. *McIntyre, D. R.,Wolff, F. G., Papachristou, C. A. & Bhunia S.* (2009) Dynamic evaluation of hardware

trust // IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 108–111. 12. *Syed Kamran Haider, Chenglu Jin, Masab Ahmad, Devu Manikantan Shila, Omer Khan and Marten van Dijk*. Advancing the State-of-the-Art // Hardware Trojans Detection, University of Connecticut, 2016. 13. *Tehranipoor, M., Wang, C*. Introduction to hardware security and trust. – New York, Springer, 2011. 14. *Banga, M.* & Hsiao, M. S. (2009) A novel sustained vector technique for the detection of hardware Trojans // in VLSI Design 2009: Improving Productivity through Higher Abstraction, The 22nd International Conference on VLSI Design, New Delhi, India, 5-9 January 2009, IEEE, pp. 327–332. 15. *Jin, Y. & Makris, Y.* (2008) Hardware Trojan detection using path delay fingerprint, in IEEE International Symposium on Hardware-Oriented Security and Trust. 16. *Potkonjak, M.* (2010) Synthesis of trustable ics using untrusted cad tools // Proceedings of the 47th Design Automation Conference, pp. 633–634. 17. *Waksman, A. & Sethumadhavan, S.* (2011) Silencing hardware backdoors // Proceedings of the 32nd IEEE Symposium on Security and Privacy, May 2011. 18. *Hicks, M., Finnicum, M., King, S. T., Martin, M. M. K. & Smith, J. M. (*2010) Overcoming an untrusted computing base: Detecting and removing malicious hardware automatically, Security and Privacy // IEEE Symposium on 0, 159–172. 19. *Silva, M. L. & Ferreira, J. C.* (2010) Creation of partial FP configurations at run-time // Proceedings of the 2010 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, DSD '10, IEEE Computer Society, Washington, DC, USA, pp. 80–87,

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 07.09.2017

УДК 004.056.55

Д.В. МЯЛКОВСКИЙ, З.А. ОРЄШКО, А.В. ПОТІЙ, д-р техн. наук

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Вступ

Наскрізне проникнення та повсякчасне зростання ступеня впливу інформаційних технологій на сучасне життя особи, бізнесу, суспільства і держави вже сьогодні вимагає чіткого визначення та правильного розуміння і застосування онтологічної моделі забезпечення електронної довіри як до електронних послуг взагалі, так до окремих етапів їх життєвого циклу зокрема.

Довіра до електронної послуги є інтегрованою характеристикою, яка буде наближатися до нижнього рівня кожного разу при встановленні невідповідності визначеним вимогам етапності, сценарію, способу, засобу або використаному джерелу інформації для її надання.

В сучасній українській термінології переважно застосовується термін «гарантія» при перекладі з англійської слова «assurance», хоча б більш правильним доцільно застосовувати термін «запевнення».

В оксфордському словнику цей англомовний термін тлумачиться «як позитивна декларація, спрямована на забезпечення довіри; обіцянка» (a positive declaration intended to give confidence; a promise). Як у звичайному просторі, так і у віртуальному ступінь довіри до об'єкта або процесу складається із сукупності показників довіри до достовірно встановленої або підтвердженої справжності кожного елемента процесу або об'єкта. Тому, чим більше таких підтверджених справжностей, тим більше кожний із нас відчуває себе впевненішим, що він не помиляється у тому, що оцінюваний об'єкт, процес тощо є справжнім, не підміненим, тотожним або є істинним за унікальним набором своїх властивостей, що відповідають або є оригіналом.

У цій статті автори аналізують предметну область електронної ідентифікації з метою уточнення змісту визначень в цій галузі.

Порівняння норм ЗУ «Про електронні довірчі послуги» та Регламент ЄС №910/2014

Алгоритми надання електронних послуг можуть і повинні відрізнятись, проте ключовим моментом тут є електронна ідентифікація. Успішне її проходження забезпечує поступове просування по ланцюгу обов'язкових кроків згідно з встановленим сценарієм надання електронної послуги. При цьому чутливим відносно довіри тут є засіб ідентифікації (довіра до повного циклу від розроблення до процесу виробництва і постачання), реалізація в ньому визначеного основного та прикладного програмного забезпечення, його захищеність від підробок, надійність механізмів захисту чутливої інформації (зокрема персональних даних), яка зберігається або використовується на конкретних етапах вказаного вище ланцюга, виконання саме встановлених сценаріїв надання послуги і так далі.

У зв'язку з цим, проблематика запровадження електронної ідентифікації набуває актуальності, особливо на тлі імплементації в Україні положень Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС (далі – Регламент-910) [1] в форматі закону України «Про електронні довірчі послуги» (№ 2155-VIII від 5 жовтня 2017 року) [2], розвитку Інтернету речей (IoT) тощо. Цей закон став логічним продовженням розвитку норм прийнятого у 2003 році Закону України «Про електронний цифровий підпис». Основна мета закону – визначити перелік електронних довірчих послуг та встановити організаційні, технологічні та інші вимоги для їх надання таким чином, щоб у одержувача цих послуг була впевненість що інфраструктура забезпечує довіру до них. Ключовим моментом в забезпеченні довіри до будь-якої електронної послуги є електронна ідентифікація суб'єкта (об'єкта) її отримання або звернення на її отримання.

Варто зазначити, що в процесі адаптації Регламенту-910 у відповідний закон належну увагу питанням електронної ідентифікації надано не було, а лише делеговано Державному агентству з питань електронного урядування України, як центральному органу виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства, здійснення розроблення нормативно-правових актів та технічне регулювання у сфері електронної ідентифікації шляхом встановлення вимог до засобів електронної ідентифікації, рівня довіри до засобів електронної ідентифікації та автентифікації для їх використання у сфері електронного урядування.

У зв'язку з неналежним висвітленням у законі питань електронної ідентифікації він і стосується, в переважному ступені, лише питань електронних довірчих послуг. При цьому, в законі уведено основні терміни та окрему статтю 6 щодо характеристик до схем ідентифікації з низьким, середнім та високим рівнем довіри до кожної з них.

Порівнюючи переклад основної термінології щодо ідентифікації, застосованої в Регламенті-910 та закону № 2155-VIII, можна спостерігати певні відмінності (табл. 1)

Таблиця 1

Норма Регламенту-910	Норма ЗУ «Про електронні довірчі послуги»
electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;	9) електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;
'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;	17) засіб електронної ідентифікації – матеріальний та/або нематеріальний об'єкт, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;
'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;	21) ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;
	22) ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на папері та/або в електронній формі, яка однозначно встановлює фізичну, юридичну особу або представника юридичної особи;
'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons	46) схема електронної ідентифікації – система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб

Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них.

Різниця між ними полягає лише в тому що, низький (середній, високий) рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений (суттєвий та найвищий відповідно) ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності.

Запроваджені Законом України «Про електронний цифровий підпис» та системою підзаконних актів механізми використання електронного цифрового підпису забезпечили впровадження та активне використання схем електронної ідентифікації в переважній

більшості з високим ступенем довіри. Водночас, ця схема, забезпечивши можливість надання юридично значущих послуг державою, почала вимагати надання належної уваги і іншим схемам, коли такий високий рівень довіри до електронної ідентифікації може бути економічно не виправданим або стримуватиме можливість розвитку інших способів, у тому числі комбінованих, способів ідентифікації, та, як наслідок, гальмування запровадження нових видів електронних послуг. При цьому забезпечення довіри до електронної ідентифікації може бути забезпечено і комбінацією інших, в тому числі організаційних, договірних тощо, механізмів.

Недостатня донедавна нормативна врегульованість питань електронної ідентифікації на тлі стрімкого розвитку сфери електронних послуг змусила як державні органи, так і розробників рішень з їх надання розробляти і впроваджувати інші схеми ідентифікації з відповідним до отримуваних електронних послуг рівнем довіри до них. Яскравим прикладом запровадження іншої схеми електронної ідентифікації стало запровадження BankID – постанова Правління Національного банку України №378 від 30 серпня 2016 року «Про затвердження Положення про Єдину національну систему електронної дистанційної ідентифікації фізичних і юридичних осіб BankID Національного банку України» [3].

Це Положення встановлює порядок функціонування Єдиної національної системи електронної дистанційної ідентифікації фізичних і юридичних осіб BankID (далі – система BankID), здійснення банками України електронної дистанційної ідентифікації клієнтів (користувачів) з метою отримання ними адміністративних послуг на Єдиному державному порталі адміністративних послуг (далі – портал) або від суб'єктів надання адміністративних послуг та доступу користувачів до інформаційно-телекомунікаційних систем державних органів. Воно є прикладом використання за встановленими правилами та способом персональних даних, які користувачем системи ідентифікації через систему BankID вже колись раніше вносились до банку, клієнтом якого є цей користувач. При цьому, критична інформація, яка містить персональні дані користувачів, перед пересиланням шифрується, а інформаційні повідомлення про результати обробки абонентами запитів на ідентифікацію підписуються електронним цифровим підписом суб'єкта, що здійснює ідентифікацію. В такій схемі більшість питань відповідальності за безпеку даних регулюється договорами між користувачами та абонентами та банками. Вимога, що встановлена Національним банком України – це дотримання вимог Положення, специфікації на підключення та наявність у абонента комплексної системи захисту інформації відповідно до законодавства України.

Іншою новою для України технологією є технологія MobileID. Ця технологія не є тільки технологією електронної ідентифікації за допомогою мобільних терміналів. Правильніше було б її розглядати як технологію, що забезпечує застосування електронного цифрового підпису (ЕЦП) за допомогою мереж мобільних телекомунікацій, у тому числі і для електронної ідентифікації та інших сервісів.

Порівняльний аналіз позначень та термінів в сфері електронної ідентифікації

Слід зазначити, що на сьогодні спостерігаються деякі відмінності у визначенні понять «ідентифікація» та «автентифікація». Якщо перший застосовується в сенсі встановлення об'єкта, то автентифікація є процесом доведення (proofing) належності або тотожності встановленого об'єкта тим рисам та характеристикам, які або раніше, або в конкретний момент часу десь наявні, тобто процес встановлення ідентичності (identity). Нижче наводиться порівняння застосованих визначень для цих понять в нормативних документах Сполучених Штатів Америки, Міжнародної організації зі стандартизації та Міжнародного Союзу Електрозв'язку та України (табл 2).

У NIST Special Publication 800-63-2 Electronic Authentication Guideline[4] визначається, що Електронна автентифікація (електронна перевірка автентичності) – це процес встановлення довіри до ідентифікацій користувачів, електронно представлених до інформаційної системи.

Електронна перевірка автентичності представляє технічну проблему, коли цей процес містить віддалену автентифікацію окремих людей через відкриту мережу з метою електронного уряду та торгівлі. Керівні принципи цього документа передбачають автентифікацію та транзакцію через відкриту мережу, таку як Інтернет.

У випадках, коли автентифікація та транзакція здійснюються через контрольовану мережу, агентства можуть враховувати таке управління безпекою як частину їх оцінки ризику.

Ця настанова надає технічні рекомендації агентствам, які дозволяють індивіду віддалено автентифікувати свою особу в Федеральній IT-системі.

Ця настанова стосується лише традиційних, широко впроваджених методів дистанційної автентифікації, яка базується на основі секретів. За допомогою цих методів індивідуум щоб бути автентифікованим доводить, що він або вона знає або володіє деякою секретною інформацією.

В цій настанові термін «ідентичність» визначено як «набір атрибутів, які однозначно описують людину в певному контексті». А термін «автентифікація» визначається як «процес встановлення довіри до ідентичності користувачів або інформаційних систем».

В міжнародному стандарті ISO/IEC 29115:2013 Information technology – Security techniques — Entity authentication assurance framework (Інформаційні технології – Методи захисту – Схеми забезпечення довіри до автентифікації суб'єктів) [6] термін «ідентичність» визначено як «набір атрибутів, пов'язаних з суб'єктом», а «автентифікація» визначений як «надання впевненості в ідентичності суб'єкта». При цьому термін «доказування ідентичності» (Identity proofing) визначено як процес, за допомогою якого провайдер цифрових послуг та орган реєстрації (ОР) збирають та перевіряють інформацію про особу з метою надання посвідчень цій особі.

В цьому стандарті термін «доказування ідентичності» визначено декілька іншим чином: «процес, за допомогою якого орган реєстрації фіксує та перевіряє достатність інформації для визначення суб'єкта до визначеного або зрозумілого рівня впевненості».

Міжнародний союз електрозв’язку випустив низку рекомендацій серії «x: Мережі даних, відкриті системи зв'язку та безпека», в яких, зокрема, також здійснюється визначення відповідних термінів.

Так, рекомендація ITU-T X.1254 «Структура забезпечення автентичності суб'єктів» [7] визначає чотири рівні підтвердження автентифікації суб'єкта (наприклад, LoA 1 – LoA 4), а також критерії та загрози для кожного з чотирьох рівнів забезпечення автентифікації організації. Крім того, він:

- визначає рамки для управління рівнем забезпечення;
- надає рекомендації щодо технологій управління, які повинні використовуватися для пом'якшення загроз автентифікації, на основі оцінки ризику;
- надає керівництво для відображення чотирьох рівнів забезпечення в інші схеми забезпечення автентичності;
- надає керівництво для обміну результатами автентифікації, які базуються на чотирьох рівнях забезпечення.

Рекомендація ITU-T X.1258 «Безпека в кіберпросторі – Управління ідентифікацією – Посилена автентифікація об'єкта на основі агрегованих (зібраних) атрибутів» [8] представляє концепцію агрегації атрибутів, яка дозволяє суб'єкту об'єднувати атрибути з декількох ідентифікаторів. Агрегація атрибутів – це механізм збору атрибутів суб'єкта, отриманого з декількох ідентифікаторів доступу.

В цій рекомендації термін «ідентичність» визначено як представлення суб'єкта у формі одного або декількох атрибутів, які дозволяють істотно розрізняти суб'єкт або об'єкти в контексті. Для цілей ідентифікації ідентифікатор розуміється як контекстна ідентичність (підмножина атрибутів), тобто різноманітність атрибутів обмежена рамкою з визначеними граничними умовами (контекстом), в яких суб'єкт існує та взаємодіє. А термін

«автентифікація» визначений як процес, який використовується для досягнення достатньої впевненості при пов’язанні між об'єктом і представленою ідентичністю.

Визначення терміну «доказування ідентичності» в цьому стандарті не спостерігається.

У нормативних документах системи технічного захисту інформації України, наприклад у НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах (КС) від несанкціонованого доступу» [9], затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 № 22, термін “автентифікація” визначений як процедура перевірки відповідності пред’явленого ідентифікатора об’єкта КС на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності. Термін «ідентичність» та «доказування ідентичності» не визначаються. Водночас визначено термін «ідентифікація» як процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання.

У табл. 2 наводяться зведені визначення термінів з цих документів.

Таблиця 2

	USA NIST Special Publication 800-63-2	**ISO/IEC**	**Рекомендація ITU-T X.1258**	**НД ТЗІ** 1.1-003-99	**НБУ**
Authentication	The process of establishing confidence in the identity of users or information systems Процес встановлення довіри до ідентичності користувачів або інформаційних систем	provision of assurance in the identity of an entity Надання впевненості в ідентичності суб'єкта **(29115:2013)** **автентифікація** (*authentication*) Забезпечення гарантії, що характеристики об'єкта, які було заявлено, є правильними **(ДСТУ ISO/IEC 27000:2015)**	**(entity) authentication** [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity. Процес, який використовується для досягнення достатньої впевненості при пов'язанні між об'єктом і представленою ідентичністю.	процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комунікаційної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності	електронний процес, що дає змогу підтвердити електронну дистанційну ідентифікацію фізичної або юридичної особи чи походження та цілісність даних в електронній формі
Identity	A set of attributes that uniquely describe a person within a given context. Identity Proofing Набір атрибутів, які однозначно описують людину в певному контексті	set of attributes related to an entity Набір атрибутів, пов'язаних з суб'єктом	**identity** [b-ITU-T X.1252]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. Представлення суб'єкта у формі одного або декількох атрибутів, які дозволяють істотно розрізняти суб'єкт або об'єкти в контексті. Для цілей ідентифікації ідентифікатор розуміється як контекстна ідентичність (підмножина атрибутів), тобто різноманітність атрибутів обмежена рамкою з визначеними граничними умовами (контекстом), в яких суб'єкт існує та взаємодіє		

Закінчення табл. 2

Identity proofing	The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. Процес, за допомогою якого провайдери сертифікації та орган реєстрації (ОР) збирають та перевіряють інформацію про особу з метою надання посвідчень цій особі	process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance Процес, за допомогою якого орган реєстрації (ОР) фіксує та перевіряє достатність інформації для визначення суб'єкта до визначеного або зрозумілого рівня впевненості			
Identification				Процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання	

Висновки

Порівняльний аналіз визначення термінів дозволяє зробити певні висновки. Існує розбіжність у визначеннях термінів «ідентифікація», «автентифікація» і пов'язаних з ними процесів в нормативних та регулюючих документах. Також неоднозначним є застосування в національних нормативних документах перекладеного терміну «assurance» не як запевнення та його міра, а як рівень гарантій.

Наслідком такої розбіжності може бути складність у застосовності норм міжнародних стандартів в нормативно-експлуатаційних документах з функціонування інформаційно-телекомунікаційних систем (ІТС), де застосовуються механізми ідентифікації та автентифікації. Складним також буде проведення в Україні оцінки відповідності таких механізмів на відповідність міжнародним стандартам або визнання в Україні результатів такої оцінки, які отримані поза межами України.

У зв'язку з цим, упровадження тотожних з міжнародною термінологію цих базових термінів та визначень в українське законодавство спростить надалі, з одного боку, реалізацію відповідних технічних механізмів в ІТС, а з іншого – можливість довіри до безпеки при їх застосуванні.

Список літератури: 1. *Регламент* (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС. 2. *Закон* України «Про електронні довірчі послуги» № 2155-VIII від 5 жовтня 2017 року. 3. *Постанова* Правління Національного банку України №378 від 30 серпня 2016 року «Про затвердження Положення про Єдину національну систему електронної дистанційної ідентифікації фізичних і юридичних осіб BankID Національного банку України» // Офіційний вісник України від 04.10.2016. – 2016. – № 76. – С. 8, ст. 2545, код акту 83254/2016. 4. *NIST* Special Publication 800-63-2. Electronic Authentication Guideline. 5. *William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W, Timothy Polk, Sarbari Gupta, Emad A. Nabb*. – U.S. Department of Commerce, National Institute of Standards and Technology, August 2013. – 112 p. 6. *ISO/IEC 29115*. Information technology. Security Techniques – entity authentication assurance framework. – ISO/IEC JTC 1/SC 27 IT Security techniques. – 2013. – 36p. 7. *Рекомендація* ITU-T X.1254 «Структура забезпечення автентичності суб'єктів» 8. *ITU-T X.1258* «Безпека в кіберпросторі – Управління ідентифікацією – Посилена автентифікація об'єкта на основі агрегованих (зібраних) атрибутів» Rec. ITU-T X.1258 (09/2016). 9. *НД ТЗІ 1.1-003-99* «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.99 № 22.

Державна служба спеціального зв'язку
та захисту інформації України,
Харківський національний
університет імені В.Н.Каразіна,
Акціонерне товариство
«Інститут інформаційних технологій»

Надійшла до редколегії 11.12.2017

УДК 681.142

В.А. КРАСНОБАЕВ, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук, В.Н. ШЛОКИН

МЕТОДЫ ОПРЕДЕЛЕНИЯ ВЫЧЕТОВ ЧИСЕЛ В КОМПЛЕКСНОЙ ЧИСЛОВОЙ ОБЛАСТИ

Введение

Повышение производительности компьютерных систем и компонент обработки целочисленных данных (КСКОЦД), функционирующих в двоичной позиционной системе счисления (ПСС), связано, прежде всего, с увеличением рабочих частот элементов и использованием моделей и методов формального синтеза, временных мультипараллельных систем и программ [1 – 3]. В то же время теоретически и практически показано, что использование непозиционной системы счисления в остаточных классах (СОК) позволяет кардинально повысить производительность и улучшить другие технические характеристики КСКОЦД [3 – 5]. Как показали исследования, важным является факт эффективного использования СОК в гиперкомплексной числовой области [6, 7].

Обобщением целых рациональных чисел являются целые комплексные (гауссовы) числа (КЧ). Целые гауссовы числа образуют кольцо: их сумма, разность и произведение также являются (как и числа в СОК) целыми гауссовыми числами. На основе свойств СОК были разработаны патентоспособные компоненты компьютерной системы обработки целочисленных данных в комплексной области [8 – 10]. В настоящее время растет интерес к непозиционной системе счисления в СОК среди разработчиков информационно-телекоммуникационных систем, реализующих процессы формирования, передачи и обработки сигналов – физических переносчиков данных, криптографического преобразования данных, сжатия видеоинформации и т. д. [11 – 19].

Цель статьи – рассмотрение методов практического определения вычетов целочисленных данных в комплексной числовой области.

Основная часть

В СОК для комплексной числовой области значения остатков КЧ представляются комплексными и вещественными вычетами по комплексным основаниям. Обработка целочисленных данных, представленных в комплексной области, основывается на результатах теоремы 1 [3].

Теорема 1. В комплексной числовой области со взаимно простыми комплексными основаниями $\dot{m}_1, \dot{m}_2, ..., \dot{m}_n$ любое представимое комплексное число $\dot{A} = a + bi$ единственным образом представляется в СОК совокупностью своих наименьших комплексных вычетов $\dot{a}_1, \dot{a}_2, ..., \dot{a}_n$ по основаниям системы.

Перед рассмотрением методов определения вычетов целочисленных данных в комплексной числовой области определим условия делимости целых КЧ [3]. Так, комплексное целое число вида $\dot{A} = a + bi$ будет считаться кратным комплексному модулю $\dot{m} = p + qi$ ($\dot{m}$ будет называться делителем числа $\dot{A}$), если частное $\frac{\dot{A}}{\dot{m}}$ является целым комплексным числом, т. е. должно выполняться условие

$$\frac{\dot{A}}{\dot{m}} = \frac{a+bi}{p+qi} = \frac{(a+bi)\cdot(p-qi)}{p^2+q^2} = \frac{a\cdot p+b\cdot q}{p^2+q^2} + \frac{b\cdot p-a\cdot q}{p^2+q^2} i. \qquad (1)$$

Очевидно, что выражение (1) будет целым КЧ, если выполняется условие

$$\begin{cases} (a\cdot p+b\cdot q) \equiv 0 \bmod (p^2+q^2), \\ (b\cdot p-a\cdot q) \equiv 0 \bmod (p^2+q^2). \end{cases} \qquad (2)$$

Пусть $\dot{S} = e + fi$ такое КЧ, что значение $\dot{A} - \dot{S}$ делится на число $\dot{m}$, тогда $\dot{S}$ является вычетом КЧ $\dot{A}$ по комплексному модулю $\dot{m}$, т.е. выполняется сравнение

$$\dot{A} \equiv \dot{S} (\mathrm{mod}\, \dot{m}), \tag{3}$$

где $N = p^2 + q^2$ – норма модуля $\dot{m} = p + qi$.

Пример 1. Определить делимость КЧ $\dot{A} = 17 + 7i$ на комплексный модуль $\dot{m} = 3 + 2i$.

Определяем следующие значения: $N = p^2 + q^2 = 3^2 + 2^2 = 13$; $a \cdot p + b \cdot q = 17 \cdot 3 + 7 \cdot 2 = 51 + 14 = 65$; $b \cdot p - a \cdot q = 7 \cdot 3 - 2 \cdot 17 = -13$. Условия (2) выполняются, т.е. $65 \equiv 0 \mathrm{mod} 13$ и $-13 \equiv 0 \mathrm{mod} 13$. Таким образом, КЧ $\dot{A} = 17 + 7i$ делится на комплексный модуль $\dot{m} = 3 + 2i$ без остатка.

Пример 2. Определить делимость КЧ $\dot{A} = 1 + i$ на комплексный модуль $\dot{m} = 1 + 2i$.

Определяем следующие значения: $N = p^2 + q^2 = 1^2 + 2^2 = 5$; $a \cdot p + b \cdot q = 1 \cdot 1 + 1 \cdot 2 = 3$ и $b \cdot p - a \cdot q = 1 \cdot 1 - 1 \cdot 2 = -1$. В этом случае, $3 \equiv 3 \mathrm{mod} 5$ и $(-1) \equiv 4 \mathrm{mod} 5$. Таким образом, имеем, что $3 \neq 4$, т.е. условия (2) не выполняются. В этом случае КЧ $\dot{A} = 1 + i$ не делится нацело на комплексный модуль $\dot{m} = 1 + 2i$, т.е. существует ненулевой остаток $x + yi$.

Метод определения комплексного вычета $x + iy$ целого комплексного числа $\dot{A} = a + bi$ по комплексному модулю $\dot{m} = p + qi$

Для понимания метода определения комплексного вычета целого комплексного числа по комплексному модулю рассмотрим следующую теорему 2 [3].

Теорема 2. Пусть даны КЧ $\dot{A} = a + bi$ и комплексный модуль $\dot{m} = p + qi$, и при этом выполняются следующие сравнения:

$$\begin{cases} (a \cdot p + b \cdot q) \equiv (x \cdot p + y \cdot q) \mathrm{mod} (p^2 + q^2), \\ (b \cdot p - a \cdot q) \equiv (y \cdot p - x \cdot q) \mathrm{mod} (p^2 + q^2). \end{cases} \tag{4}$$

Тогда $\dot{A} = (x + yi) \mathrm{mod}\, \dot{m}$, т.е. значение $x + yi$ является комплексным вычетом КЧ $\dot{A}$ по комплексному модулю $\dot{m}$.

Доказательство. Делим КЧ $\dot{A} - (x + yi)$ на модуль $\dot{m} = p + qi$. Получим

$$\frac{\dot{A} - (x + yi)}{\dot{m}} = \frac{(a - x) + (b - y)i}{p + qi} = \frac{[(a - x) + (b - y)i]}{p^2 + q^2} =$$

$$= \frac{(a - x) \cdot p + (b - y) \cdot q}{p^2 + q^2} + \frac{(b - y) \cdot p - (a - x) \cdot q}{p^2 + q^2} i.$$

Для того чтобы в результате операции деления получилось целое КЧ, должно иметь место сравнение

$$\begin{cases} [(a - x) \cdot p + (b - y) \cdot q] \equiv 0 \mathrm{mod} (p^2 + q^2), \\ [(b - y) \cdot p - (a - x) \cdot q] \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{5}$$

Или

$$\begin{cases} (a \cdot p - x \cdot p + b \cdot q - y \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2), \\ (b \cdot p - y \cdot p - a \cdot q - x \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{6}$$

Из (6) имеем, что

$$\begin{cases} [(a \cdot p + b \cdot q) - (x \cdot p + y \cdot q) \equiv 0 \mathrm{mod} (p^2 + q^2), \\ [(b \cdot p - a \cdot q) - (y \cdot p - x \cdot q)] \equiv 0 \mathrm{mod} (p^2 + q^2). \end{cases} \tag{7}$$

Сравнение (7) эквивалентно сравнению (4). Что и требовалось доказать. Таким образом,

число $x+yi$ является вычетом КЧ $\dot{A}=a+bi$ по модулю $\dot{m}=p+qi$.

Метод определения комплексного вычета состоит в решении сравнений (4) путем реализации совокупности операций, входящих в сравнения (7).

Приведем конкретные примеры определения $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$

Пример 3. Определить вычет $x+yi$ числа $\dot{A}=15+2i$ по модулю $\dot{m}=3+2i$ ($N=p^2+q^2=9+4=13$). В соответствии с выражением (4) запишем систему сравнений в виде

$$\begin{cases}(15\cdot 3+2\cdot 2)\equiv(3x+2y)\bmod 13,\\ 2\cdot 3-15\cdot 2\equiv(3y-2x)\bmod 13.\end{cases}$$

Или

$$\begin{cases}49\equiv(3x+2y)\bmod 13,\\ -24\equiv(3y-2x)\bmod 13.\end{cases}$$

В этом случае имеем систему из двух сравнений с двумя неизвестными вида

$$\begin{cases}3x+2y\equiv 49\bmod 13,\\ 3y-2x\equiv -24\bmod 13.\end{cases}$$

С учетом того, что $49(\bmod 13)=10$ и $-24(\bmod 13)=2$ получим систему из двух линейных уравнений

$$\begin{cases}3x+2y=10,\\ -2x+3y=2.\end{cases}$$

Решение этой системы из двух линейных уравнений будет состоять из двух значений $x=2$ и $y=2$. В этом случае искомый вычет (результат) $x+yi$ равен числу $x+yi=2+2i$. Таким образом, вычет $x+yi$ КЧ $\dot{A}=15+2i$ по модулю $\dot{m}=3+2i$ равен $x+yi=2+2i$. Или можно записать результат решения в виде сравнения $(15+2i)\equiv(2+2i)\bmod(3+2i)$.

Пример 4. Определить вычет $x+yi$ числа $\dot{A}=1+i$ по модулю $\dot{m}=1+2i$ ($N=p^2+q^2=1+4=5$).

В соответствии с (4) составим и решим систему сравнений

$$\begin{cases}(1\cdot 1+1\cdot 2)\equiv(x\cdot 1+y\cdot 2)\bmod 5,\\ (1\cdot 1-1\cdot 2)\equiv(y\cdot 1-x\cdot 2)\bmod 5.\end{cases}$$

$$\begin{cases}(x+2\cdot y)\equiv 3(\bmod 5),\\ (-2\cdot x+y)\equiv -1(\bmod 5).\end{cases}$$

$$\begin{cases}x+2\cdot y\equiv 3(\bmod 5),\\ -2\cdot x+y\equiv 4(\bmod 5).\end{cases}$$

$$\begin{cases}x+2\cdot y=3,\\ -2\cdot x+y=4.\end{cases}$$

$$x=3-2\cdot y,$$

$$-2\cdot(3-2\cdot y)+y=4,$$

$$-6+4y+y=4,$$

$$5\cdot y=10,$$

$$y=2.$$

$$x = 3 - 2 \cdot y,$$

$$x = 3 - 2 \cdot 2 = -1 (\mathrm{mod}\, 5),$$

$$x = 4.$$

Таким образом: $(x + yi) = 4 + 2i$, т.е. $\dot{A} = (x + yi) \bmod \dot{m}$. Или результат можно записать в виде сравнения $(1+i) \equiv (4+2i) \bmod (1+2i)$.

Пример 5. Определить вычет $x + yi$ числа $\dot{A} = 15 + 2i$ по модулю $\dot{m} = 1 + 2i$ ($N = 5$; $a = 15$, $b = 2$; $p = 1$, $q = 2$).

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases} (15 \cdot 1 + 2 \cdot 2) \equiv (x \cdot 1 + 2 \cdot y) \bmod 5, \\ (2 \cdot 1 - 15 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

$$\begin{cases} 19 \equiv (x + 2 \cdot y) \bmod 5, \\ (-28) \equiv (-2 \cdot x + y) \bmod 5. \end{cases}$$

Систему сравнений представим как систему из двух линейных уравнений

$$\begin{cases} x + 2 \cdot y = 19, \\ -2 \cdot x + y = -28. \end{cases}$$

Решение системы уравнений будет представлено в виде $x = 15$, $y = 2$. Т.е. решение $\dot{A} \equiv (x + yi) \bmod \dot{m}$ представится в виде $(15 + 2i) \equiv (15 + 2i) \bmod (1 + 2i)$.

Пример 6. Найти комплексный вычет $x + yi$ комплексного числа $\dot{A} = 2 + i$ по комплексному модулю $\dot{m} = 1 + 2i$.

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases} (2 \cdot 1 + 1 \cdot 2) \equiv (x \cdot 1 + y \cdot 2) \bmod 5, \\ (1 \cdot 1 - 2 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

Или

$$\begin{cases} 4 \equiv (x + 2y) \bmod 5, \\ (-3) \equiv (y - 2x) \bmod 5. \end{cases}$$

На основании системы сравнений составим и решим систему двух линейных уравнений

$$\begin{cases} x + 2 \cdot y = 19, \\ -2 \cdot x + y = 2, \end{cases}$$

$$x = 4 - 2y,$$

$$-2 \cdot (4 - 2y) + y = 2,$$

$$-8 + 4y + y = 2,$$

$$5y = 10,$$

$$y = 2.$$

В этом случае $x = 4 - 2y = 4 - 4 = 0$, а вычет (остаток) равен $x + yi = 0 + 2i = 2i$. Т.е. результат $x + yi = 2i$ решения сравнения $\dot{A} \equiv (x + yi) \bmod \dot{m}$ можно представить следующим образом: $(2 + i) \equiv (2i) \bmod (1 + 2i)$.

Метод определение наименьшего комплексного вычета $x+iy$ комплексного числа $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$

Известно, что для КЧ не определены понятия "больше" и "меньше". Однако в математике представляется возможным формально (например, формально полагают, что $0!=1$) определить понятие наименьшего комплексного вычета по комплексного модулю. Основная идея такого определения состоит в том, что поскольку определение комплексного вычета распространяется на системы вещественных сравнений (4), то потребовав, чтобы $x\cdot p+y\cdot q$ и $y\cdot p-x\cdot q$ были соответственно наименьшими вычетами по модулю $N=p^2+q^2$, получим вполне определенное КЧ $x+yi$, которое формально можно назвать наименьшим вычетом числа $\dot{A}$ по модулю $\dot{m}$, т.е. предполагается, что

$$\begin{aligned} x\cdot p+y\cdot q &\le p^2+q^2-1,\\ y\cdot p-x\cdot q &\le p^2+q^2-1. \end{aligned} \tag{8}$$

При этом различают наименьшие вычеты и абсолютно наименьшие вычеты. В первом случае предполагается, что $x\cdot p+y\cdot q$ и $y\cdot p-x\cdot q$ являются натуральными числами, не превосходящими значения p^2+q^2-1. Во втором случае предполагается, что эти величины могут быть как положительными, так и отрицательными, но не превосходящими по абсолютной величине значения $\frac{p^2+q^2}{2}$ [3].

Если найдены наименьшие вычеты выражений

$$\begin{cases} \Gamma=(a\cdot p+b\cdot q)\bmod(p^2+q^2);\\ \Gamma'=(b\cdot p-a\cdot q)\bmod(p^2+q^2), \end{cases} \tag{9}$$

то наименьший вычет числа $\dot{A}$ по модулю $\dot{m}$

$$x+yi=\frac{\Gamma\cdot p-\Gamma'\cdot q}{p^2+q^2}+\frac{\Gamma'\cdot p+\Gamma\cdot q}{p^2+q^2}i, \tag{10}$$

где Γ и Γ' – наименьшие положительные вычеты по вещественному модулю $N=p^2+q^2$; Γ и Γ' могут принимать значения вещественных чисел $0,1,...,N-1$.

Согласно (4) получаем систему из 2-х линейных сравнений с двумя неизвестными:

$$\begin{cases} \Gamma\equiv(x\cdot p+y\cdot q)\bmod(p^2+q^2);\\ \Gamma'\equiv(y\cdot p-x\cdot q)\bmod(p^2+q^2). \end{cases} \tag{11}$$

Как и ранее, наименьший вычет $x+yi$ числа $\dot{A}=a+bi$ по модулю $\dot{m}=p+qi$ равен и обозначается как $(a+bi)\equiv(x+yi)\bmod\dot{m}$. Установлено, что наименьший вычет $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$ определяется исходя из решения системы двух вещественных сравнений (11).

Приведем конкретные примеры определения наименьшего вычета $x+yi$ любого КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$.

Пример 7. Определить наименьший вычет $x+yi$ числа $\dot{A}=15+2i$ по модулю $\dot{m}=1+2i$ ($a=15$, $b=2$; $p=1$, $q=2$; $N=p^2+q^2=1^2+2^2=5$).

По формуле (10) определим значение $x+yi$, где значения Γ и Γ' определяются в соответствии с формулой (9):

$$\Gamma=(a\cdot p+b\cdot q)\bmod N=(15\cdot1+2\cdot2)\bmod5=19(\bmod5)=4;$$

$$\Gamma'=(b\cdot p-a\cdot q)\bmod N=(2\cdot1-15\cdot2)\bmod5=(-28)\bmod5=(-3)\bmod5=2.$$

По формуле (10) определяем наименьший вычет $x+yi$, т.е.

$$x+yi=\frac{\Gamma\cdot p+\Gamma'\cdot q}{N}+\frac{\Gamma'\cdot p+\Gamma\cdot q}{N}i=\frac{4\cdot 1-2\cdot 2}{5}+\frac{2\cdot 1+4\cdot 2}{5}i=2i\,.$$

Пример 8. Определить наименьший вычет $x+yi$ КЧ $\dot{A}=15+2i$ по комплексному модулю $\dot{m}=3+2i$ ($a=15,\ b=2;\ p=3,\ q=2;\ N=p^2+q^2=13$).

Определим значения Γ и Γ' (формула (9))

$$\Gamma=(15\cdot 3+2\cdot 2)\bmod 13=49(\bmod 13)=10\,;$$

$$\Gamma'=(2\cdot 3-15\cdot 2)\bmod 13=(-24)\bmod 13=(-11)\bmod 13=2\,.$$

Наименьший вычет $x+yi$ определяется в соответствии с формулой (10)

$$x+yi=\frac{10\cdot 3-2\cdot 2}{13}+\frac{2\cdot 3+10\cdot 2}{13}i=2+2i\,.$$

Отметим, что исходя из соотношений (9), между значениями Γ и Γ' существует аналитическая зависимость. Установим данную зависимость, необходимую для использования ее при определения наименьшего вычета $x+yi$ КЧ $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$. Для этого умножим первое сравнение (11) на p, а второе на число q. Получим следующую совокупность сравнений

$$\Gamma\cdot p\equiv p\cdot(x\cdot p+y\cdot q)\bmod(p^2+q^2)\,,$$
$$\Gamma'\cdot q\equiv q\cdot(y\cdot p-x\cdot q)\bmod(p^2+q^2).$$

После этого производим вычитание второго сравнения из первого

$$(\Gamma\cdot p-\Gamma'\cdot q)\equiv\left[p\cdot(x\cdot p+y\cdot q)-q\cdot(y\cdot p-x\cdot q)\right]\bmod(p^2+q^2)\,.$$

Получим следующее сравнение

$$(\Gamma\cdot p-\Gamma'\cdot q)\equiv(p^2\cdot x+p\cdot y\cdot q-q\cdot y\cdot p+q^2\cdot x)\bmod(p^2+q^2)$$

или

$$x\cdot(p^2+q^2)\equiv(\Gamma\cdot p-\Gamma'\cdot q)\bmod(p^2+q^2)\,.$$

В итоге имеем, что

$$\Gamma'\cdot q\equiv\Gamma\cdot p\bmod(p^2+q^2)\,. \qquad (12)$$

В [3] показано, что если p и q – взаимно простые числа (НОД $(\mathrm{p,q})=1$), то сравнение (12) имеет одно решение:

$$\Gamma'\equiv t\cdot\Gamma\bmod N\,, \qquad (13)$$

где $t=\frac{p+z\cdot(p^2+q^2)}{q}$, причем z таково, что $t<N$ – целое число, меньшее значения нормы N. Величина t определяется подбором (перебором) соответствующего значения z.

Метод определения наименьшего комплексного вычета $x+iy$ комплексного числа $\dot{A}=a+bi$ по комплексному модулю $\dot{m}=p+qi$ состоит в определении значения (10), путем реализации совокупности операций при решении сравнений (11).

Пример 9. Определить все возможные пары значений Γ и Γ' при модуле $\dot{m}=p+qi=1+2i$. Определить значения Γ' из сравнения $\Gamma'\equiv(t\cdot\Gamma)\bmod N$ для $\dot{m}=p+qi=1+2i$ (формула (13)).

В этом случае $t=\frac{p+z\cdot N}{q}$, при этом $z<N$ – целое число. Для данного модуля $\dot{m}=p+qi=1+2i$ имеем, что

$$t=\frac{p+z\cdot(p^2+q^2)}{q}=\frac{1+z\cdot(1+4)}{2}=\frac{1+z\cdot 5}{2}=\frac{1+1\cdot 5}{2}=3.$$

Очевидно, что значение t будет целым числом в случае, когда $z=1$, т.е. в этом случае $t=3$. Рассчитанные значения Γ и Γ' даны в табл. 1.

Таблица 1

Γ	$\Gamma'\equiv(3\cdot\Gamma)\bmod 5$ $(t=3)$	Γ	$\Gamma'\equiv(3\cdot\Gamma)\bmod 5$ $(t=3)$
0	0	3	4
1	3	4	2
2	1	–	–

В соответствии с полученными результатами и на основании выражения (10) определим наименьшие комплексные вычеты $x+yi$ КЧ $a+bi$ по комплексному модулю $\dot{m}=1+2i$ (где $\Gamma=\overline{1,N-1}$).

$\Gamma=0;\ \Gamma'=0.\ x+yi=\frac{0}{5}+\frac{0}{5}=0+0i=0;$

$\Gamma=1;\ \Gamma'=3.\ x+yi=\frac{1\cdot 1-3\cdot 2}{5}+\frac{3\cdot 1+1\cdot 2}{5}i=-1+i;$

$\Gamma=2;\ \Gamma'=1.\ x+yi=\frac{2\cdot 1-1\cdot 2}{5}+\frac{1\cdot 1+2\cdot 2}{5}i=i;$

$\Gamma=3;\ \Gamma'=4.\ x+yi=\frac{3\cdot 1-4\cdot 2}{5}+\frac{4\cdot 1+3\cdot 2}{5}i=-1+2i;$

$\Gamma=4;\ \Gamma'=2.\ x+yi=\frac{4\cdot 1-2\cdot 2}{5}+\frac{2\cdot 1+4\cdot 2}{5}i=2i.$

В табл. 2 представлена совокупность наименьших комплексных вычетов по модулю $\dot{m}=1+2i$.

Таблица 2

Γ	Γ'	x	y	Наименьшие вычеты x+yi
0	0	0	0	0
1	3	-1	1	-1+i
2	1	0	1	i
3	4	-1	2	-1+2i
4	2	0	2	2i

Пример 10. Определить все возможные пары значений Γ и Γ' для модуля $\dot{m}=p+qi=3+4i$. $N=3^2+4^2=25$. Так как НОД (3, 4)=1, то в данном случае имеем, что

$$t=\frac{p+z\cdot N}{q}=\frac{3+1\cdot 25}{4}=7.$$

В соответствии с (13), имеем $\Gamma'\equiv 7\cdot\Gamma(\bmod 25)$, что и определяет возможные пары чисел Γ и Γ' (табл. 3).

Таблица 3

Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$	Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$	Г	$\Gamma' \equiv (7 \cdot \Gamma) \bmod 25$
0	0	9	13	18	1
1	7	10	20	19	8
2	14	11	2	20	15
3	21	12	9	21	22
4	3	13	16	22	4
5	10	14	23	23	11
6	17	15	5	24	18
7	24	16	12	–	–
8	6	17	19	–	–

Метод определения вещественного вычета h целого комплексного числа $\dot{A} = a + bi$ по комплексному модулю $\dot{m} = p + qi$

В СОК есть возможность представить комплексные числа в образе их вещественных вычетов, т.е. установить изоморфизм между комплексными и вещественными вычетами чисел. Это дает возможность заменить арифметические операции над целыми гауссовыми числами аналогичными операциями над системой вещественных чисел по вещественным модулям, равным нормам выбранных комплексных оснований СОК. В этом аспекте существует такая актуальная задача, как преобразование остатков числа в СОК из комплексной числовой области в вещественную числовую область. Данная задача преобразования числа в СОК из комплексной числовой области в вещественную область решается путем использования результатов первой фундаментальной теореме Гаусса.

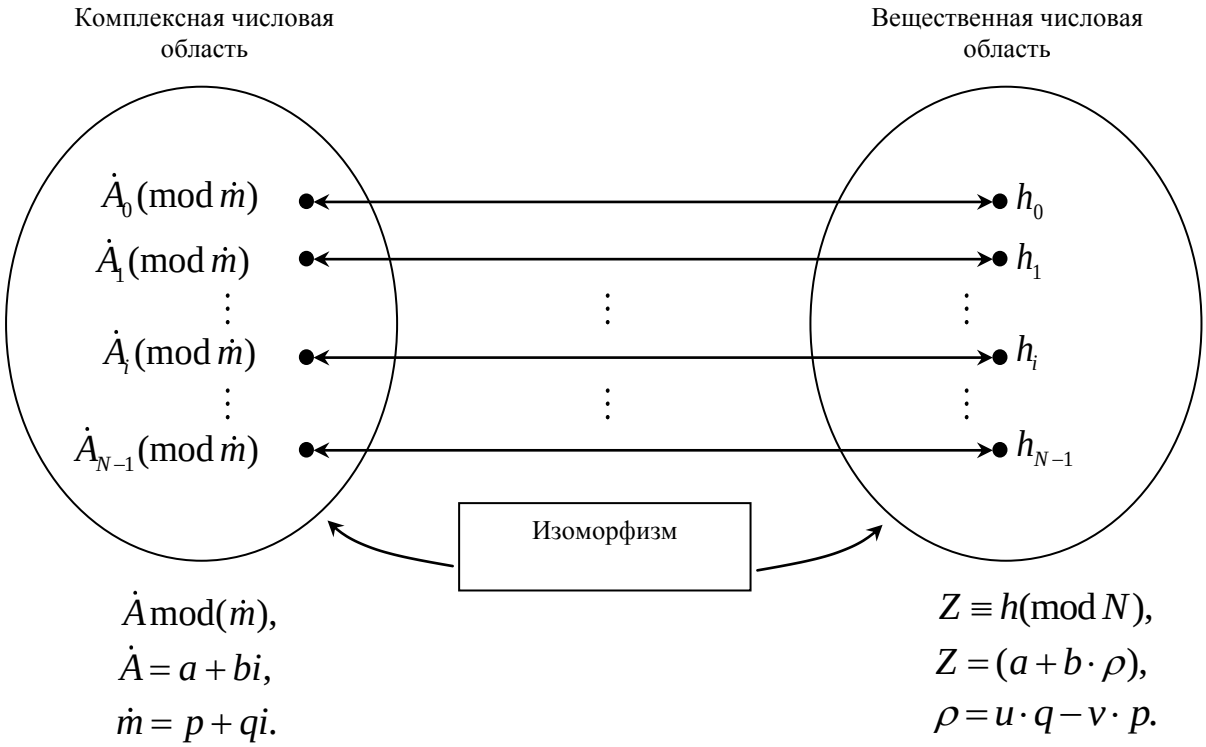
Первая фундаментальная теорема Гаусса

Здесь мы подошли к одному из наиболее интересных и важных вопросов теории целых комплексных чисел – к определению класса наименьших вычетов и связанной с этим первой фундаментальной теоремой Гаусса об изоморфизме между множеством вещественных и комплексных вычетов чисел.

Изложенный материал подводит к первой фундаментальной теореме Гаусса. Теорема 3 устанавливает изоморфизм между комплексными и вещественными вычетами.

Теорема 3. По заданному комплексному модулю $\dot{m} = p + qi$, норма N которого равна $N = p^2 + q^2$ и для которого p и q являются взаимно простыми числами, каждое целое КЧ $\dot{A} = a + bi$ по комплексному модулю $\dot{m}$ сравнимо с одним и только одним вещественным вычетом из ряда чисел $\overline{0, N-1}$, т.е. имеем, что $\dot{A} \equiv h(\bmod \dot{m})$.

На рисунке представлена схема соответствия произвольного комплексного вычета $\dot{A} \ (\bmod \dot{m})$ вещественному h вычету $\mathrm{Z} \equiv h(\bmod N)$.



Доказательство. Из теории чисел известно, что для двух взаимно простых чисел p и q можно найти такие два целых числа u и v, что выполняется условие

$$u \cdot p + v \cdot q = 1. \tag{14}$$

Покажем справедливость следующего тождества:

$$i = u \cdot p - v \cdot q + \dot{m} \cdot (v + ui). \tag{15}$$

Действительно

$$\begin{aligned} i &= u \cdot q - v \cdot p + (p + q \cdot i) \cdot (v + u \cdot i) = \\ &= u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i + q \cdot u \cdot i^2) = \\ &= u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i - q \cdot u) = \\ &= u \cdot q - q \cdot u - v \cdot p + p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i = \\ &= (u \cdot p + v \cdot q) \cdot i. \end{aligned}$$

С учетом выражения (14) имеем, что $i = i$. Таким образом тождество (15) справедливо.
Пусть дано КЧ $\dot{A} = a + bi$. Тогда с учетом (15) получим

$$\begin{aligned} a + bi &= a + b \cdot [u \cdot q - v \cdot p + \dot{m} \cdot (v + ui)] = \\ &= a + (u \cdot q - v \cdot p) \cdot b + \dot{m} \cdot (v \cdot b + u \cdot bi)]. \end{aligned} \tag{16}$$

Обозначим через h наименьший положительный вещественный вычет числа $a + (u \cdot q - v \cdot p) \cdot b$ по модулю N, т.е.

$$h \equiv [a + (u \cdot q - v \cdot p) \cdot b] \mathrm{mod}\, N. \tag{17}$$

Запишем выражение (17) в виде равенства

$$a + (u \cdot q - v \cdot p) \cdot b = h + s \cdot N. \tag{18}$$

Или запишем равенство (18) в виде

$$h + s \cdot N = h + s(p + qi) \cdot (p - qi) = h + \dot{m} \cdot (p \cdot s - q \cdot si). \tag{19}$$

Тогда, с учетом (16), будет выполняться равенство

$$a+bi = h+\dot{m}\cdot(p\cdot s-q\cdot si)+\dot{m}\cdot(v\cdot b+u\cdot bi) = \\ = h+\dot{m}\cdot\left[p\cdot s+v\cdot b+(u\cdot b-q\cdot s)i\right],$$

или в форме сравнения

$$(a+bi)\equiv h(\mathrm{mod}\,\dot{m}).$$

Таким образом, доказано, что наименьший комплексный вычет $x+yi$ КЧ $a+bi$ сравним по модулю m с одним и только одним из вещественных чисел $0, 1, 2, ..., N-1$.

Докажем, методом от противного, что это вещественное число единственное. Допустим, что имеются два сравнения:

$$(a+bi)\equiv h_1(\mathrm{mod}\,\dot{m}),$$
$$(a+bi)\equiv h_2(\mathrm{mod}\,\dot{m}).$$

На основании свойства сравнений имеем

$$h_1\equiv h_2(\mathrm{mod}\,\dot{m})$$

или

$$(h_1-h_2)\equiv 0(\mathrm{mod}\,\dot{m}),$$

т. е. $(h_1-h_2)=\dot{m}\cdot(e+f\cdot i)$. (20)

Из (20) следует выполнение равенства ($\dot{m}=p+qi$):

$$(h_1-h_2)=(p+qi)\cdot(e+fi).$$

Умножим обе части этого равенства на величину $p-q\cdot i$. Получим, что

$$(h_1-h_2)\cdot(p-qi)=(p+qi)\cdot(p-qi)\cdot(e+fi),$$
$$(h_1-h_2)\cdot(p-qi)=(p^2+q^2)\cdot(e+fi),$$
$$(h_1-h_2)\cdot(p-qi)=N\cdot(e+fi),$$
$$(h_1-h_2)\cdot p-(h_1-h_2)\cdot qi=N\cdot e+N\cdot fi.$$

Последнее выражение эквивалентно следующим двум вещественным равенствам:

$$\begin{cases}(h_1-h_2)\cdot p=N\cdot e,\\(h_1-h_2)\cdot q=-N\cdot f.\end{cases} \quad (21)$$

Так как КЧ равны между собой, то равны и их вещественные и мнимые части. Умножив первое равенство (21) на u и второе – на v и потом сложим их. Получим

$$(h_1-h_2)\cdot(u\cdot p+v\cdot q)=N\cdot(e\cdot u-f\cdot v).$$

Принимая во внимание выражение (14) ($u\cdot p+v\cdot q=1$) следует, что

$$(h_1-h_2)\equiv N\cdot(e\cdot u-f\cdot v),$$

или

$$(h_1-h_2)\equiv 0(\mathrm{mod}\,N). \quad (22)$$

Так как по предположению $h_1, h_2 < N$, то сравнение (22) возможно только в случае $h_1=h_2$. Таким образом, исключается возможность существования двух различных чисел h_1 и h_2, меньших N, которые были бы сравнимы с числом $a+bi$ по модулю $\dot{m}$. Имеется только одно такое h число, которое определяется из сравнения (17) и представляется в виде сравнения

$$[a+(u\cdot q-v\cdot p)\cdot b]\equiv h(\mathrm{mod}\,N). \qquad (23)$$

При этом используется обозначение $\mathrm{Z}=(a+b\cdot\rho)$, где выражение $\rho=u\cdot q-v\cdot p$, посредством которого устанавливается соответствие между комплексным и вещественным вычетом по модулю $\dot{m}=p+qi$, называется коэффициентом изоморфизма (КИ). В этом случае выражение (23) представится в виде

$$\mathrm{Z}\equiv h(\mathrm{mod}\,N). \qquad (24)$$

На основании данных табл. 2 по формулам (23) и (24) определим значения вещественных вычетов $Z_i\equiv h_i(\mathrm{mod}\,N)$ $(i=\overline{0,N-1})$, соответствующих наименьшим комплексным вычетам $x+yi$ по модулю $\dot{m}=1+2i$. Вначале определим значение коэффициента изоморфизма $\rho=u\cdot q-v\cdot p=u\cdot 2-v\cdot 1$. Значения u и v определяются из известного в теории чисел соотношения $u\cdot p+v\cdot q=1$, т.е. $u\cdot 1+v\cdot 2=1$. Путем подбора (перебора) определяем, что $u=-1$, а $q=1$. Таким образом, $\rho=(-1)\cdot 2-1\cdot 1=-3$, или $(-3)\,\mathrm{mod}\,5=2$ $(N=p^2+q^2=1^2+2^2=5)$.

Определим исходные значения наименьших вещественных вычетов h_i, изоморфных наименьшим комплексным вычетам, представленных в табл. 2.

Для $\dot{A}=0+0i$. $Z_0=a+b\rho=0+0\cdot\rho=0$. $h_0\equiv 0(\mathrm{mod}\,5)$.

Для $\dot{A}=-1+i$. $Z_1=-1+1\cdot(-3)=-4$. $h_1\equiv 1(\mathrm{mod}\,5)$.

Для $\dot{A}=i$. $Z_2=0+1\cdot(-3)=-3$. $h_2\equiv 2(\mathrm{mod}\,5)$.

Для $\dot{A}=-1+2\cdot i$. $Z_3=-1+2\cdot(-3)=-1-6=-7$. $h_3\equiv 3(\mathrm{mod}\,5)$.

Для $\dot{A}=2\cdot i$. $Z_4=0+2\cdot(-3)=-6$. $h_3\equiv 4(\mathrm{mod}\,5)$.

Результаты вычислений наименьших вещественных значений остатков (вычетов) h_i сведены в табл. 4.

Таблица 4

Наименьшие комплексные вычеты x+yi	КИ	Значение $Z_i=a+b\cdot\rho$	Вещественные вычеты $h_i(Z_i\equiv h_i(modN);\ i=\overline{0,N-1}$
0	2	0	0
-1+i	2	-4	1
i	2	-3	2
-1+2i	2	-7	3
2i	2	-6	4

На основе результатов теоремы Гаусса нетрудно показать следующее соотношения между наименьшими комплексными и вещественными вычетами. Пусть для двух чисел $\dot{A}_1=a_1+b_1i$ и $\dot{A}_2=a_2+b_2i$ существуют такие значения чисел h_1 и h_2, $h_\pm$ и $h_\times$, что если $\dot{A}_1\equiv h_1(\mathrm{mod}\,\dot{m})$ и $\dot{A}_2\equiv h_2(\mathrm{mod}\,\dot{m})$, то выполняются соотношения $\dot{A}_1\pm\dot{A}_2\equiv h_\pm(\mathrm{mod}\,\dot{m})$ и $\dot{A}_1\cdot\dot{A}_2\equiv h_\times(\mathrm{mod}\,\dot{m})$. Тогда $h_\pm\equiv(h_1\pm h_2)\,\mathrm{mod}\,N$ и $h_\times\equiv(h_1\cdot h_2)\,\mathrm{mod}\,N$, где $N=p^2+q^2$.

Приведем примеры решения сравнений в комплексной области, т.е. примеры определение наименьших вещественных вычетов h комплексных чисел $\dot{A}=a+bi$ по комплексным модулям $\dot{m}=p+qi$.

Пример 11. Решить сравнение $(16+7i)\equiv h\,\mathrm{mod}(5+2i)$. Т.е. необходимо найти наименьший вещественный вычет h комплексного числа $16+7i$ по комплексному модулю $5+2i$.

Поскольку НОД $(5,2)=1$, то условие первой фундаментальной теоремы Гаусса выполня-

ется, следовательно, существует полная система вещественных вычетов по модулю $N = p^2 + q^2 = 5^2 + 2^2 = 29$. Вещественный вычет h определяется из сравнения (24), т.е.

$$(16 + 7 \cdot \rho) \equiv h (\mathrm{mod}\, 29).$$

Коэффициент изоморфизма $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 5$. Значения u и v определяются из условия равенства (14) подбором значений u, v. Определили, что $u = 1$ и $v = -2$. Проверка соотношения (14) показала, что $1 \cdot 5 + (-2) \cdot 2 = 5 - 4 = 1$.

В этом случае КИ $\rho = 1 \cdot 2 - (-2) \cdot 5 = 2 + 10 = 12$. Поэтому $Z = 16 + 7 \cdot \rho = 16 + 7 \cdot 12 = 100$. Решим сравнение $100 \equiv h (\mathrm{mod}\, 29)$ и получим $h \equiv 13 (\mathrm{mod}\, 29)$. В общем виде можно записать, что $16 + 7i \equiv 13 \mathrm{mod}(5 + 2i)$.

Пример 12. Решить сравнение $(1 + i) \equiv h \,\mathrm{mod}(1 + 2i)$. Или, необходимо найти наименьший вещественный вычет h комплексного числа $1 + i$ по комплексному модулю $1 + 2i$.

В этом случае НОД $(p, q) = (1, 2) = 1$. $N = p^2 + q^2 = 1 + 2^2 = 5$. $\dot{A} \equiv h (\mathrm{mod}\, \dot{m})$. $h \equiv (a + b \cdot \rho) \bmod N$.

Значение КИ $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1$, а значения u и v определяются из соотношения (14)

$$u \cdot p + v \cdot q = 1, \qquad u \cdot 1 + v \cdot 2 = 1, \text{ т.е.} \qquad u = -1,\ v = 1.$$

Таким образом $\rho = (-1) \cdot 2 - 1 \cdot 1 = -2 - 1 = -3$.

$$h = 1 + 1 \cdot 2 = 3.$$
$$x + yi = 4 + 2i \;\square\; h = 3,$$
$$\text{т.е. } (1 + i) \equiv 3 \mathrm{mod}(1 + 2i).$$

Рассмотрим примеры 13 и 14 определения комплексного и вещественного вычетов целого комплексного числа по комплексному модулю $\dot{m} = 1 + 2i$ с контролем правильности решения задачи. Исходные данные для контроля представлены в табл. 5.

Таблица 5

Г	$\Gamma' = 3 \cdot \Gamma (\mathrm{mod}\, 5)$, $(t = 3)$	Наименьшие комплексные вычеты $x + yi$ по комплексному модулю $\dot{m} = 1 + 2i$ комплексного числа $\dot{A} = a + bi$	Вещественные вычеты h по модулю $N = p^2 + q^2 = 5$
0	0	$0 + 0i$	0
1	3	$-1 + i$	1
2	1	i	2
3	4	$-1 + 2i$	3
4	2	$2i$	4

Пример 13А. Определить комплексный вычет $x + yi$ КЧ $\dot{A} = 1 + i$ по комплексному модулю $\dot{m} = 1 + 2i$, т.е. найти $\dot{A} \equiv (x + yi) \bmod \dot{m}$ ($a = 1$, $b = 1$; $p = 1$, $q = 2$; $N = 5$). По формуле (4) имеем, что

$$\begin{cases} (1 \cdot 1 + 1 \cdot 2) \equiv (x \cdot 1 + y \cdot 2) \bmod 5, \\ (1 \cdot 1 - 1 \cdot 2) \equiv (y \cdot 1 - x \cdot 2) \bmod 5. \end{cases}$$

$$\begin{cases} 3 = x + 2y, \\ -1 = -2x + y. \end{cases}$$

$$x = 3 - 2y,$$
$$-1 = -2 \cdot (3 - 2y) + y,$$
$$-1 = -6 + 4y + y,$$
$$5y = 5,$$
$$y = 1.$$
$$x = 3 - 2y = 3 - 2 = 1;\ x = 1.$$

Ответ: комплексный вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен комплексному числу $x+yi=1+i$.

Пример 13Б. Определить наименьший вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$, т.е. определить значение $1+i\equiv(x+yi)\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$). По формуле (10) имеем, что

$$\Gamma=(1\cdot1+1\cdot2)\bmod5=3;\ \Gamma'=(1\cdot1-1\cdot2)\bmod5=(-1)\bmod5=4.$$

$$x+yi=\frac{3\cdot1-4\cdot2}{5}+\frac{4\cdot1+3\cdot2}{5}i=-\frac{5}{5}+\frac{10}{5}i=-1+2i.$$

Таким образом, наименьший вычет $x+yi$ КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен значению $x+yi=-1+2i$. Это решение можно представить в виде $(1+i)\equiv(-1+2i)\bmod(1+2i)$.

Пример 13В. Решить сравнение $\dot{A}\equiv h\bmod\dot{m}$ вида $(1+i)\equiv h\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$), формулы (14), (23), (24))

$$u\cdot p+v\cdot q=1,\ u=-1,$$
$$u\cdot1+v\cdot2=1.\ v=1.$$
$$\rho=u\cdot q-v\cdot p.$$
$$Z=a+b\cdot\rho,$$
$$Z\equiv h\bmod N.$$
$$\rho=(-1)\cdot2-1\cdot1=-2-1=-3.$$
$$Z=1+1\cdot(-3)=-2.$$
$$\mathrm{h}\equiv(-2)\bmod5=3.$$

Таким образом, вещественный вычет h КЧ $\dot{A}=1+i$ по комплексному модулю $\dot{m}=1+2i$ равен величине $h=3$.

Проверка. Проведем проверку полученных результатов. В примере 13Б получили наименьший комплексный вычет $(-1+2i)$, а в примере 13В получим вещественный вычет $h=3$. В соответствии с данными табл. 5 имеем, что $(-1+2i)\sim3$. Что и требовалось показать.

Пример 14А. Определить комплексный вычет $x+yi$ КЧ $\dot{A}=3+4i$ по комплексному модулю $\dot{m}=1+2i$. $N=p^2+q^2=1^2+2^2=5$.

В соответствии с выражением (4) составим систему сравнений в виде

$$\begin{cases}(3\cdot1+4\cdot2)\equiv(x\cdot1+y\cdot2)\bmod5,\\(4\cdot1-3\cdot2)\equiv(y\cdot1-x\cdot2)\bmod5.\end{cases}$$

Или

$$\begin{cases}11\equiv(x+2y)\bmod5,\\(-2)\equiv(-2x+y)\bmod5.\end{cases}$$

На основании системы сравнений составим систему из двух линейных уравнений

$$\begin{cases}x+2y=11,\\-2x+y=+3,\end{cases}$$

так, как $(-2)=3\bmod5$.

$$x=11-2y,$$
$$-2\cdot(11-2\cdot y)+y=3,$$
$$-22+4y+y=3,$$
$$5y=25,$$
$$y=5.$$

$$x = 11 - 2y = 11 - 10 = 1.$$

Таким образом, имеем, что комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$ равен значению $x + yi = 1 + 5i$.

Пример 14Б. Определить наименьший комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$. $N = 5$.

В соответствии с выражением (10) имеем, что наименьший комплексный вычет равен значению

$$(x + yi) = \frac{\Gamma \cdot p - \Gamma' \cdot q}{N} + \frac{\Gamma' \cdot p + \Gamma \cdot q}{N} i.$$

Предварительно определим значения Γ и Γ' (см. формулы (9)):

$$\Gamma = (a \cdot p + b \cdot q) \bmod N = (3 \cdot 1 + 4 \cdot 2) \bmod 5 = 11 (\bmod 5) = 1;$$
$$\Gamma' = (b \cdot p - a \cdot q) \bmod N = (4 \cdot 1 - 3 \cdot 2) \bmod 5 = (-2) \bmod 5 = 3.$$

В этом случае имеем, что

$$(x + yi) = \frac{1 \cdot 1 - 3 \cdot 2}{5} + \frac{3 \cdot 1 + 1 \cdot 2}{5} = -\frac{5}{5} + \frac{5}{5} = -1 + i.$$

Таким образом, наименьший комплексный вычет $x + yi$ КЧ $\dot{A} = 3 + 4i$ по комплексному модулю $\dot{m} = 1 + 2i$ равен значению $-1 + i$.

Пример 14В. Определить вещественный вычет h КЧ $\dot{A} = 3 + 4i$ по модулю $\dot{m} = 1 + 2i$. $N = 5$. Или можно сформулировать задачу следующим образом. Решить сравнение вида $(3 + 4i) \equiv h \bmod (1 + 2i)$.

В соответствии с выражением (24) имеем, что $(a + b\rho) \equiv h (\bmod N)$, где КИ $\rho = u \cdot q - v \cdot p$. На основе формулы (14) определим значения u и v

$$u \cdot p + v \cdot q = 1 \text{ или } u \cdot 1 + v \cdot 2 = 1.$$

Так, при значениях $u = -1$ и $v = 1$ выполните условие (14), т.е. $(-1) \cdot 1 + 1 \cdot 2 = 1$.

На основании расчетов получим, что $\rho = u \cdot q - v \cdot p = (-1) \cdot 2 - 1 \cdot 1 = -3$.

$$\mathrm{Z} = (a + b \cdot \rho) = 3 + 4 \cdot (-3) = -9.$$

Имеем $(a + b\rho) \equiv h (\bmod N)$ или $(-9) \equiv 1 (\bmod 5)$. Т.е. $h = 1$.

Таким образом, имеем решение сравнения в виде $(3 + 4i) \equiv 1 \bmod (1 + 2i)$.

Проверка. В примере 14Б получили наименьший комплексный вычет $(-1 + i)$, а в примере 14В получим вещественный вычет $h = 1$. В соответствии с данными табл. 5 имеем, что $(-1 + i) \sim 1$. Что и требовалось показать.

Выводы

Рассмотрены методы:

- определения комплексного вычета целого комплексного числа по комплексному модулю;
- определения наименьшего комплексного вычета целого комплексного числа по комплексному модулю;
- определения вещественного вычета целого комплексного числа по комплексному модулю, основанный на использование результатов первой фундаментальной теоремы Гаусса.

Приведены конкретные примеры определения вычетов целочисленных данных в комплексной числовой области. На основании представленных методов разработано устройство для их технической реализации [20]. На устройство получен патент Украины на изобретение,

что подтверждает новизну и практическую ценность результатов исследований. Выводы и результаты, полученные в статье, целесообразно использовать при реализации задач и алгоритмов в СОК для комплексной числовой области. Использование представленных методов способствует повышению эффективности использования СОК для быстрой реализации целочисленных операций в комплексной числовой области.

Список литературы: 1. *Синтез* и анализ параллельных процессов в адаптивных времяпараметризованных вычислительных системах / Г. А. Поляков, С. И. Шматков, Е. Г, Толстолужская, Д. А. Толстолужский. – Харьков : ХНУ им. В. Н. Каразина, 2012. -672с. *2. Филиппенко И. Г.* Взаимодействующие нейроавтоматы и нейроавтоматно-вычислительные структуры : под ред. О. Г. Руденко. – К. : Каравелла, 2015, 440 с. *3. Акушский И. Я., Юдицкий Д. И.* Машинная арифметика в остаточных классах. – М. : Сов. радио, 1968. – 440 с. *4. Krasnobayev V. A., Koshman S. A., Mavrina M. A.* A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. – November 2014. – Volume 50, Issue 6, pp 969-976. 5. *Krasnobayev V. A., Yanko A. S., Koshman S.* A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150. *6. Карл Фридрих Гаусс.* Труды по теории чисел. – М. : Академия наук СССР, 1959. – 979 с. 7. *Применение* гиперкомплексных чисел в теории инерциальной навигации. Автономные системы / Онищенко С. М. – Киев : Наук. думка, 1983. - 208с. 8. *ДП* на корисну модель № 33672 України, МПК G 06 F 7/49 (2008.01) / Кошман С.О., Сіора О.А., Хері Алі Абдуллах, Краснобаєв В.А. Пристрій для множення комплексних чисел у модулярній системі числення; № u 2008 01356. Заявл. 04.02.2008. Опубл. 10.07.2008, Бюл. № 13. – 8с. 9. *ДП* на корисну модель № 40905 України, МПК G 06 F 7/00 (2009) / Кошман С.О., Барсов В.І., Сіора О.А., Краснобаєв В.А. Пристрій для піднесення комплексних чисел в квадрат за комплексним модулем у модулярній системі числення. № u 2008 14308. Заявл. 12.12.2008. Опубл. 27.04.2009, Бюл. № 8.-5с. 10. *ДП* на корисну модель № 33672 України, МПК G 06 F 7/49 (2008.01) / Кошман С.О., Сіора О.А., Хері Алі Абдуллах, Краснобаєв В.А. Пристрій для множення комплексних чисел у модулярній системі числення; № u 2008 01356. Заявл. 04.02.2008. Опубл. 10.07.2008, Бюл. № 13.-8с. 11.*Kuznetsov, O., Gorbenko, Y., Kolovanova, I.* Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58. DOI: 10.1109/INFOCOMMST.2016.7905334. 12. *Kuznetsov, O., Lutsenko, M., Ivanenko, D.* Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62. DOI: 10.1109/INFOCOMMST.2016.7905335. 13. *Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A., Berezovsky, A.* The statistical analysis of a network traffic for the intrusion detection and prevention systems // Telecommunications and Radio Engineering. – Volume 74, 2015, Issue 1, pages 61-78. DOI: 10.1615/TelecomRadEng.v74.i1.60. *Karpenko O., Kuznetsov A., Sai V., Stasev Yu.* Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. – Volume 71, 2012 Issue 1. pages 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100. 14. *Yuriy Izbenko, Vladislav Kovtun, Alexandr Kuznetsov.* The design of boolean functions by modified hill climbing method // Information technology – New Generation, 2009. ITNG'2009. Proceedings of the 6th International Conference on Information Technology: New Generations, April 27-29, Las Vegas, Nevada, USA., pp: 356-361. DOI: 10.1007/s10559-007-0052-8. 15. *Naumenko, N.I., Stasev, Yu.V., Kuznetsov, A.A.* Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326. DOI: 10.1007/s10559-007-0052-8. *Stasev Yu.V., Kuznetsov A.A., Nosik A.M.* Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11. DOI: 10.1007/s10559-007-0021-2. 16. *Stasev Yu. V., Kuznetsov A.A.* Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363. DOI: 10.1007/s10559-005-0069-9. 17. *I. D. Gorbenko, A. G. Kachko, K. A. Pogrebnyak, L. V. Makutonin* Analysis, assessment and proposals regarding the method for generation of system parameters in ntru-like asymmetric systems // Telecommunications and Radio Engineering, Volume 76, 2017, p. 511-520. DOI: 10.1615/ TelecomRadEng.v76.i6.50. 18. *T. O. Grinenko, O. P. Narezhniy, I. D. Gorbenko* Methods for measuring the noise power spectral density of the random number generator quantum radio optical system // Telecommunications and Radio Engineering, Volume 76, 2017, pages 635-651 DOI: 10.1615/TelecomRadEng.v76.i7.60. 19. *Gorbenko I.D., Zamula A.A., Semenko Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. pages 169–178. 20. *Патент* на винахід № 114063, Україна, МПК G 06 F 7/72 (2006.01), H 03 M 7/18 (2006.01). Краснобаєв В. А., Горбенко І. Д., Янко А. С., Кошман С. А., Мороз С. О., Горбенко Ю. І Пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів. № a 2016 06697. Заявл. 21.06.2016. Опубл. 10.04.2017, Бюл. № 7. – 7с.

Харьковский национальный
университет имени В.Н.Каразина

Поступила в редколлегию 11.12.2017

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 621.396

В.К. ВОЛОСЮК, д-р техн. наук, С.С. ЖИЛА, канд. техн. наук,
В.В. ПАВЛІКОВ, д-р техн. наук, А.Д. АБРАМОВ, канд. техн. наук, В.Г. ЯКОВЛЕВ

ОПТИМАЛЬНЫЙ АЛГОРИТМ ОЦЕНКИ РАДИОЯРКОСТИ В ПРОСТРАНСТВЕННО-РАСПРЕДЕЛЕННЫХ РАДИОМЕТРИЧЕСКИХ СИСТЕМАХ

Введение

Радиометрические системы используют при решении задач дистанционного зондирования Земли, пассивной радиолокации, метеорологии, радионавигации и медицины. Такое широкое применение связано с высокой информативностью собственного радиотеплового излучения, энергоэффективностью и малыми массо-габаритными характеристиками аппаратуры. Простейшим устройством оценки пространственного распределения радиояркости является радиометр со сканирующей антенной, угловое разрешение которого определяется линейными размерами апертуры антенны. В практике радиометрических измерений можно добиться более высокого разрешения за счет применения пространственно-распределенных систем с нелинейной многоканальной обработкой − систем апертурного синтеза [1 − 6]. В основу разработки таких систем положена теорема Ван Циттерта − Цернике [7], связывающая угловое распределение радиояркости и функцию взаимной пространственной когерентности посредством многомерного преобразования Фурье. Алгоритм синтезирования апертуры в радиометрических система основан на корреляционной теории и не был получен из решения оптимизационной задачи статистического синтеза таких систем. Представляет интерес получить оптимальный алгоритм оценки радиояркости в пространственно-распределенных
радиометрических системах методом максимального правдоподобия и разработать соответствующие технические решения для его реализации.

Уравнение наблюдения

Сигналы, наблюдаемые с выходов линейных частей (ЛЧП) пространственно-распределенных приемников, имеют вид:

$$\vec{u}_{\sum}(t,\vec{r}') = \| u_{k\sum}(t,\vec{r}') \| = \vec{u}_s(t,\vec{r}',\vec{\lambda}) + \vec{u}_n(t,\vec{r}') + \vec{n}_p(t,\vec{r}'), \quad (1)$$

где $\vec{u}_s(t,\vec{r}',\lambda) = \| u_{ks}(t,\vec{r}',\vec{\lambda}) \| = \| u_{kD}(t,\vec{r}',\vec{\lambda}) \| + \| u_{k\phi}(t,\vec{r}') \|$, $\vec{u}_n(t,\vec{r}') = \| u_{kn}(t,\vec{r}') \|$,

$\vec{n}_p(t,\vec{r}') = \| n_{kp}(t,\vec{r}') \|$, $k = \overline{1,K}$, $\vec{r}' = (x',y') \in D'$, $t \in (0,T)$.

Все функции в (1) считаем однородными в пространстве и стационарными во времени случайными гауссовыми процессами. Индекс k означает набор независимых уравнений на разных поляризациях, частотных поддиапазонах, необходимых для оценок нескольких параметров.

Спектр (1) ограничен по частоте частотной характеристикой ЛЧП $\dot{K}_k(j2\pi f)$, а сектор принимаемых углов диаграммой направленности единичной антенны $\dot{F}_A(\vec{\vartheta}-\vec{\vartheta}_0, f)$. На ширину $\dot{K}_k(j2\pi f)$ не налагаются никакие ограничения.

Принятый полезный сигнал $u_{ks}(t,\vec{r}',\vec{\lambda})$ характеризуется спектрально-угловой плотностью комплексной амплитуды

$$\dot{A}_{ks}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})] = \dot{K}_k(j2\pi f)\dot{F}_A(\vec{\vartheta}-\vec{\vartheta}_0, f)\,\dot{A}_{ok}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})], \quad (2)$$

где $\vec{\vartheta}_0$ – направление максимума диаграммы направленности; $\dot{A}_{ok}(\vec{\vartheta}, f, \vec{\lambda}) = \dot{A}_{kD}(\vec{\vartheta}, f, \vec{\lambda}) + \dot{A}_{k\Phi}(\vec{\vartheta}, f)$ – спектрально-угловая плотность комплексной амплитуды на входе антенной системы, содержащая полезное $\dot{A}_{kD}(\vec{\vartheta}, f, \vec{\lambda})$ и фоновое $\dot{A}_{k\Phi}(\vec{\vartheta}, f)$ излучения.

Основной оцениваемый параметр, яркость излучения, представим следующим образом:

$$B_{ks}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})] = |\dot{K}_k(i2\pi f)|^2 \, |\dot{F}_A(\vec{\vartheta} - \vec{\vartheta}_0, f)|^2 \, B_{ok}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})], \quad (3)$$

$$B_{ok}(\vec{\vartheta}, f, \vec{\lambda}) = B_{kD}(\vec{\vartheta}, f, \vec{\lambda}) + B_{k\Phi}(\vec{\vartheta}, f). \quad (4)$$

Внутренние шумы приемников $\vec{u}_n(t, \vec{r}') = \| u_{kn}(t, \vec{r}') \|$ – это дельта-коррелированные шумы на выходе ЛЧП с корреляционной функцией

$$R_{ku_n}(t_1 - t_2, \vec{r}_1' - \vec{r}_2') = \langle u_{kn}(t_1, \vec{r}_1) u_{kn}(t_2, \vec{r}_2) \rangle = 0{,}5 N_{0k} H_k(t_1 - t_2) \delta(\vec{r}_1' - \vec{r}_2'), \quad (5)$$

где $H_k(t_1 - t_2) = F^{-1}[|K_k(j2\pi f)|^2]$.

Задача восстановления пространственного распределения радиояркости относится к классу обратных задач и требует регуляризации. В качестве регуляризационной добавки в (1) вводятся белые гауссовы шумы $\vec{n}_p(t, \vec{r}') = \| n_{kp}(t, \vec{r}') \|$ с корреляционными функциями $R_{kp}(t_1 - t_2) = (N_{0kp}/2)\delta(t_1 - t_2)\delta(\vec{r}_1' - \vec{r}_2')$.

Искомые спектральные яркости $\vec{\lambda}(\vec{\vartheta}) = B_{ks}(\vec{\vartheta}, f, \vec{\lambda})$ источников излучения связаны с корреляционными функциями $R_{ku_s}(\Delta\vec{r}', \tau, \vec{\lambda})$ преобразованиями V_F и V_F^{-1} [8]:

$$f^{-2} c^2 B_{ks}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})] = V_F[R_{ku_s}(\Delta\vec{r}', \tau, \vec{\lambda})] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} R_{ku_s}(\Delta\vec{r}', \tau, \vec{\lambda}) \exp\{-j2\pi f (\tau + \frac{\vec{\vartheta}\Delta\vec{r}'}{c})\} d\tau d\vec{\rho}', \quad (6)$$

$$R_{ku_s}(\Delta\vec{r}', \tau, \vec{\lambda}) = <[u_{ks}(\vec{r}_1', t_1) u_{ks}(\vec{r}_2', t_2)]> = V_F^{-1}\{B_{ks}[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})]\} =$$

$$= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} B_{ks}\left[\vec{\vartheta}, f, \vec{\lambda}(\vec{\vartheta})\right] \exp\left\{ j2\pi f (\tau + c^{-1}\vec{\vartheta}\,\Delta\vec{r}') \right\} df \, d\vec{\vartheta}. \quad (7)$$

Данные преобразования, в отличие от теоремы Ван Циттерта – Цернике, не имеют ограничения на широкоплосность сигнала и позволяют синтезировать системы, когда условие пространственно-временной узкополосности (ПВУ), или, что то же самое, условие квазимонохроматического приближения (КМП) [8, 9], не выполняется.

Решение оптимизационной задачи

Оптимизацию алгоритмов оценки радиояркости $\vec{\lambda}(\vec{\vartheta}) = B_{ks}[\vec{\vartheta}]$ выполним методом максимального правдоподобия в результате решения следующего уравнения:

$$\sum_{k=1}^{K} \int_T \int_T \int_{D'} \int_{D'} \frac{\delta R_{k\Sigma}[t_1, t_2, \vec{r}_1', \vec{r}_2', \vec{\lambda}(\vec{\vartheta})]}{\delta\lambda_j(\vec{\vartheta})} W_{k\Sigma}[t_2, t_1, \vec{r}_2', \vec{r}_1', \vec{\lambda}(\vec{\vartheta})] dt_1 dt_2 d\vec{r}_1' d\vec{r}_2' \Rightarrow$$

$$\Rightarrow \sum_{k=1}^{K} \int_T \int_T \int_{D'} \int_{D'} \frac{\delta W_{k\Sigma}[t_1, t_2, \vec{r}_1', \vec{r}_2', \vec{\lambda}(\vec{\vartheta})]}{\delta\lambda_j(\vec{\vartheta})} u_{k\Sigma}(t_1, \vec{r}_1') u_{k\Sigma}(t_2, \vec{r}_2') dt_1 dt_2 d\vec{r}_1' d\vec{r}_2', \quad (8)$$

где $\delta R_{k\Sigma}/\delta\lambda_j$, $\delta W_{k\Sigma}/\delta\lambda_j$ – операторы вариационных производных, $\Rightarrow$ – знак приравнивания. Левая часть (8) является математическим ожиданием правой.

Решение (8) имеет вид

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{f_2^4}{c^4} \int_{-\infty}^{\infty} \frac{|\dot{K}_k(j2\pi f_1)\dot{F}_A(\vec{\vartheta}_1 - \vec{\vartheta}_0, f_1)|^2}{B_{k\Sigma}(f_2, \vec{\vartheta}_2, \vec{\lambda}(\vartheta_2))} \left| \dot{\Psi}(f_1 - f_2, (f_1\vec{\vartheta}_1 - f_2\vec{\vartheta}_2)c^{-1}) \right|^2 d\vec{\vartheta}_2 df_1 df_2 \Rightarrow$$

$$\Rightarrow \int_{-\infty}^{\infty} \frac{f_1^4}{c^4} \left|\dot{K}_k(j2\pi f_1)\dot{F}_A(\vec{\vartheta}_1-\vec{\vartheta}_0, f_1)\right|^2 B_{k\Sigma}^{-2}(f,\vec{\vartheta}_1,\vec{\lambda}(\vec{\vartheta}_1))\left|\dot{S}_{kTD'}(j2\pi f_1\vec{\vartheta}_1)\right|^2 df_1, \qquad (9)$$

где $|\dot{S}_{kTD'}(j2\pi f_1\vec{\vartheta}_1)|^2$ – V_F периодограмма, усеченная интервалами наблюдения T и D', $\dot{\Psi}(f_1-f_2,(f_1\vec{\vartheta}_1-f_2\vec{\vartheta}_2)c^{-1})$ – функция неопределенности, $B_{k\Sigma}[f,\vec{\vartheta},\vec{\lambda}(\vec{\vartheta})]=B_{ks}[f,\vec{\vartheta},\vec{\lambda}(\vec{\vartheta})]+$ $+\frac{f^2}{c^2}\frac{N_{0k}}{2}\left|\dot{K}_k\left(j2\pi f\right)\right|^2+\frac{f^2}{c^2}\frac{N_{0kp}}{2}$.

Правая часть (9) показывает основные операции обработки радиотеплового излучения и структуру пространственно-распределенной радиометрической системы. Основная операция здесь – формирование V_F -периодограммы, которая заключается в фильтрации принимаемых процессов по временным частотам f, фазовой задержке каждой частотной составляющей на величину $2\pi f\vec{\vartheta}\vec{r}'/c$ и синфазном суммировании задержанных сигналов по всем элементам антенной решетки. Еще одной оптимальной операцией является адаптивная декорреляция сформированной периодограммы. Декоррелирующий фильтр содержит функцию, обратную спектральной яркости $B_{k\Sigma}[f,\vec{\vartheta},\vec{\lambda}(\vec{\vartheta})]$.

Усреднение декоррелированных колебаний путем их интегрирования по частотам f обеспечивает состоятельность оценок радиояркостных изображений $B_{0k}\left(\vec{\vartheta}\right)$ и параметров $\vec{\lambda}(\vec{\vartheta})$. С одной стороны, декорреляция уменьшает радиусы корреляции усредняемых процессов, увеличивая число их независимых отсчетов в пространственно-временной области по переменной t и координатам $\vec{r}'$, что повышает эффективность усреднения при интегрировании возведенных в квадрат декоррелированных процессов. С другой стороны, расширение полосы декоррелирующих фильтров, характеризующихся множителем при периодограмме, обеспечивает интегрирование большего числа ее некоррелированных отсчетов в спектральной области по частотам f.

Техническая реализация алгоритма (9) на практике затруднительна. Введем ряд допущений для разработки квазиоптимальных структур радиометрических систем.

Квазиоптимальные алгоритмы формирования оценки радияркости

Рассмотрим более подробно функцию неопределенности:

$$\dot{\Psi}(f_1-f_2,\, f_1\vec{\vartheta}_1-f_2\vec{\vartheta}_2)=\dot{\Psi}_T(f_1-f_2)\dot{\Psi}_{D'}(f_1\vec{\vartheta}_1-f_2\vec{\vartheta}_2)=$$

$$=TX'_mY'_m\,\mathrm{sinc}[\pi(f_1-f_2)T]\,\mathrm{sinc}[\pi(f_1\vartheta_{1x}-f_2\vartheta_{2x})c^{-1}X'_m]\times\mathrm{sinc}[\pi(f_1\vartheta_{1y}-f_2\vartheta_{2y})c^{-1}Y'_m]. \qquad (10)$$

Эта функция определяет совместную разрешающую способность системы по частотам f и направлениям $\vec{\vartheta}$. В случае приема узкополосного излучения на частоте f_0 функция $\dot{\Psi}_{D'}[f_0(\vec{\vartheta}_1-\vec{\vartheta}_2)]$ соответствует диаграмме направленности раскрыва D' с постоянным в его пределах АФР. Разрешающая способность по частотам имеет порядок $1/T$, где T – время наблюдения. Это время может быть очень большим (сотни миллисекунд, секунды и более) и потенциальная разрешающая способность по частотам может быть очень большой.

1. *Обработка сигналов в широкополосных системах апертурного синтеза*. Для широкополосных и сверхширокополосных систем, полосы частот которых составляют от сотен мегагерц до нескольких гигагерц, множитель $\dot{\Psi}_T(f_1-f_2)$, определяющий разрешающую способность по частоте, является узким и в его пределах функции $B_{k\Sigma}(f_2,\vec{\vartheta}_2,\vec{\lambda}(\vartheta_2))$, $\dot{\Psi}_{D'}(f_1\vec{\vartheta}_1-f_2\vec{\vartheta}_2)$ и f_2^4 практически постоянны, вынесем их за знак интеграла по f_2 в точке f_1. Тогда система уравнений (9) примет следующий вид:

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{f_1^4}{c^4}\frac{|\dot K_k(j2\pi f_1)\dot F_A(\vec\vartheta_1-\vec\vartheta_0,f_1)|^2}{B_{k\Sigma}(f_1,\vec\vartheta_2,\vec\lambda(\vartheta_2))}|\dot\Psi_{D'}[f_1(\vec\vartheta_1-\vec\vartheta_2)]|^2\,d\vec\vartheta_2 df_1\Rightarrow$$

$$\Rightarrow\frac{1}{T}\int_{-\infty}^{\infty}\frac{f_1^4}{c^4}\frac{|\dot K_k(j2\pi f_1)\dot F_A(\vec\vartheta_1-\vec\vartheta_0,f_1)|^2}{B_{k\Sigma}^2(f,\vec\vartheta_1,\lambda(\vec\vartheta_1))}\left|\dot S_{kTD'}(j2\pi f_1\vec\vartheta_1)\right|^2 df_1=\frac{1}{T}Y_{вых\,k}(\vec\vartheta_1). \qquad (11)$$

Множитель

$$\frac{f_1^4}{c^4}\frac{\left|\dot K(j2\pi f_1)\dot F_A(\vec\vartheta_1-\vec\vartheta_0,f_1)\right|^2}{B_{k\Sigma}^2(f,\vec\vartheta_1,\lambda(\vec\vartheta_1))}=\left|\dot L_k[j2\pi f,\vec\vartheta_1,\lambda(\vec\vartheta_1]\right|^2$$

отвечает за пространственно-временную декорреляцию наблюдаемого процесса. Декорреляция является адаптивной, т. к. зависит от величин оцениваемых параметров $\vec\lambda(\vec\vartheta_1)$. Выбрав некоторое среднее значение $\vec\lambda(\vec\vartheta_1)\approx\vec\lambda_0$, т.е. исключив адаптацию, умножив числитель и знаменатель в левой части системы (11) на $B_{k\Sigma}(f_1,\vec\vartheta_2,\vec\lambda_0)$, получим

$$\int_{-\infty}^{+\infty}B_{0k}[f_0,\vec\vartheta_2,\vec\lambda(\vec\vartheta_2)]\Psi_{kw}(\vec\vartheta_1,\vec\vartheta_2)d\vec\vartheta_2\Rightarrow$$

$$\Rightarrow\frac{1}{T}\int_{-\infty}^{+\infty}\left|\dot L_k[j2\pi f,\vec\vartheta_1,\vec\lambda_0]\right|^2\left|\dot S_{kTD'}(j2\pi f,\vec\vartheta_1)\right|^2 df-\Sigma B=\frac{1}{T}\int_0^T\left|u_{kD'_w}(t,\vec\vartheta)\right|^2 dt-\Sigma B, \qquad (12)$$

где

$$\Sigma B=B_{wn_k}+B_{wn_{kp}}=\frac{N_{0k}}{2}\int_{-\infty}^{+\infty}\frac{f^2}{c^2}\left|\dot L_k[j2\pi f,\vec\vartheta_1,\vec\lambda_0]\right|^2\left|\dot K_k(j2\pi f)\right|^2\int_{-\infty}^{+\infty}\left|\dot\Psi_{D'}[f(\vec\vartheta_1-\vec\vartheta_2)]\right|^2 d\vec\vartheta_2 df+$$

$$+\frac{N_{0kp}}{2}\int_{-\infty}^{+\infty}\frac{f^2}{c^2}\left|\dot L_k[j2\pi f,\vec\vartheta_1,\vec\lambda_0]\right|^2\int_{-\infty}^{+\infty}\left|\dot\Psi_{D'}[f(\vec\vartheta_1-\vec\vartheta_2)]\right|^2 d\vec\vartheta_2 df,$$

$$u_{kD'_w}(t,\vec\vartheta)=\int_{D'}u_{kw}\left(t-\vec\vartheta\vec r'c^{-1},\vec r'\right)d\vec r', \qquad (13)$$

$$u_{kw}(t-\vec\vartheta\vec r'c^{-1},\vec r')=\int_T h_{kw}(t-\tau)u_{k\Sigma}(\tau-\vec\vartheta\vec r'c^{-1},\vec r')d\tau,$$

$$h_{kw}(t)=F^{-1}\left\{\dot L_k[j2\pi f,\vec\vartheta_1,\vec\lambda_0]\right\}. \qquad (14)$$

Суть алгоритма (12) заключается в следующем:

1) задержка колебаний $u_{k\Sigma}(t,\vec r')$ в каждом элементе антенной системы с координатами $\vec r'$ и формирование синфазных (в соответствии с наклоном фронта поля $u_{ks}(t,\vec r')$) колебаний $u_{k\Sigma}(\tau-\vec\vartheta\vec r'c^{-1})$ для каждого направления $\vec\vartheta$;

2) декорреляция колебания $u_{k\Sigma}(\tau-\vec\vartheta\vec r'c^{-1})$ в фильтре с импульсной характеристикой $h_{kw}(t)$;

3) синфазное интегрирование задержанных и декоррелированных колебаний (для дискретных АР – сложение) и формирование сигналов $u_{kD'_w}(t,\vec\vartheta)$;

4) формирование сигналов, пропорциональных средней мощности синфазно проинтегрированных колебаний, полученных для каждого направления $\vec\vartheta$ в отдельности;

5) устранение смещения на величину ΣB.

Полученным алгоритмическим операциям соответствует структурная схема на рис. 1.

В левой части системы уравнений показан физический смысл формирования оценки радиояркости − свертка истинной радиояркости с функцией неопределенности. Функция

$\Psi_{kw}(\vec{\vartheta}_1,\vec{\vartheta}_2)$ сглаживает по переменной $\vec{\vartheta}$ функции $B_{0k}(\vec{\vartheta})$ и $\lambda(\vec{\vartheta})$, а также определяет качество и, прежде всего, разрешающую способность воспроизведения спектральной яркости $B_{0k}(\vec{\vartheta})$.

Следует отметить, что классической является функция неопределенности Вудворта, определяющая совместную разрешающую способность радиолокатора по дальности и скорости и связанные с ними длительность импульса и ширину спектра, находящиеся между собой в обратной зависимости. Такая функция неопределенности похожа по своему физическому смыслу на соотношение неопределенности Гейзенберга в квантовой механике. Но в последнее время часто функциями неопределенности стали называть аппаратные функции, определяющие разрешающие способности систем и по пространственным, в частности угловым, координатам, что, возможно, не совсем корректно. Для функций, характеризующих разрешающую способность по многим переменным (по дальности, скорости, угловым координатам и др.), вероятно, такое определение может быть приемлемым.

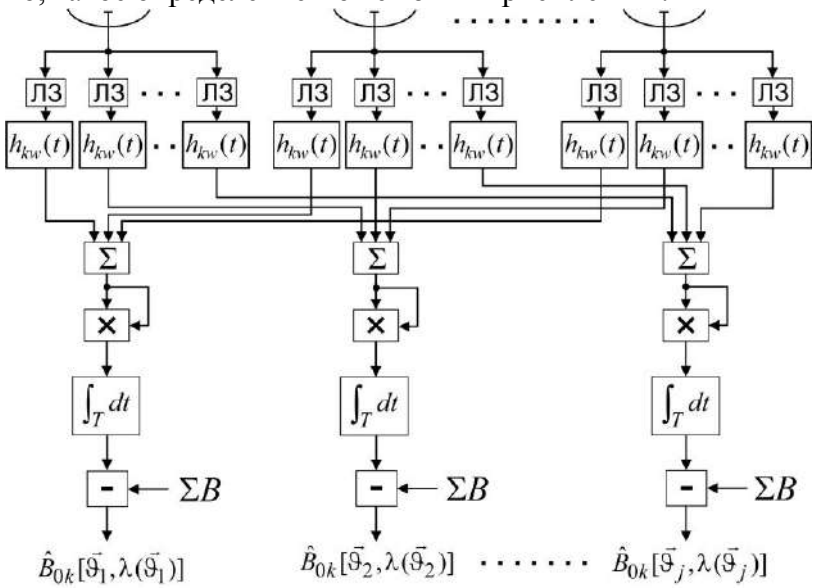


Рис. 1. Структурная схема формирования радиояркостного изображения в пространственно-распределенных радиометрических системах

2. *Обработка сигналов в узкополосных системах апертурного синтеза.* Если в заданной полосе частот $\dot{\Psi}_{D'}[f(\vec{\vartheta}_1-\vec{\vartheta}_2)\approx\dot{\Psi}_{D'}[f_0(\vec{\vartheta}_1-\vec{\vartheta}_2)$ и $\dot{F}_A(\vec{\vartheta}_2-\vec{\vartheta}_0,f)\approx\dot{F}_A(\vec{\vartheta}_2-\vec{\vartheta}_0,f_0)$, то, вынося за знак интеграла попеременной f эти множители в (12), приходим к упрощенной системе оценок радиояркостей $\hat{B}_{ok}[f_0,\vec{\vartheta}_2,\hat{\vec{\lambda}}(\vec{\vartheta}_2)]$ и параметров $\hat{\vec{\lambda}}(\vec{\vartheta}_2)$:

$$\hat{B}_{ok}[f_0,\vec{\vartheta}_2,\hat{\vec{\lambda}}(\vec{\vartheta}_2)]=\int\limits_{-\infty}^{+\infty}B_{ok}[f_0,\vec{\vartheta}_2,\vec{\lambda}(\vec{\vartheta}_2)]\left|\dot{\Psi}_{D'}[f_0(\vec{\vartheta}\ -\vec{\vartheta}_2)]\right|^2 d\vec{\vartheta}_2\approx$$

$$\approx\frac{\int\limits_0^T\left|u1_{kD'_w}(t,\vec{\vartheta})\right|^2 dt}{T\Delta F_{kw}\left(\vec{\vartheta},\vec{\lambda}_0\right)\left|\dot{F}_A(\vec{\vartheta}_1-\vec{\vartheta}_0,f_0)\right|^2}-\Sigma B1, \qquad (15)$$

где

$$\Delta F_{kw}\left(\vec{\vartheta},\vec{\lambda}_0\right)=\int\limits_{-\infty}^{+\infty}\left|\dot{L}_{k1}[j2\pi f,\vec{\vartheta},\vec{\lambda}_0]\right|^2\left|\dot{K}(j2\pi f))\right|^2 df=\int\limits_{-\infty}^{\infty}\frac{f^4}{c^4}\frac{\left|\dot{K}(j2\pi f\ ))\right|^4}{B_{k\Sigma}^2(f,\vec{\vartheta}_1,\vec{\lambda}_0)}df, \qquad (16)$$

$$\left|\dot{L}_{k1}[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]\right|^2=\frac{\left|\dot{L}_k[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]\right|^2}{\left|\dot{F}_A(\vec{\vartheta}_1-\vec{\vartheta}_0,f)\right|^2}=\frac{f^4}{c^4}\frac{\left|\dot{K}(j2\pi f)\right|^2}{B_{k\Sigma}^2(f,\vec{\vartheta}_1,\vec{\lambda}_0)}. \quad (17)$$

Смещение оценок радияркостей $\Sigma B1$ вычисляется в (12) с указанными выше упрощениями по тем же формулам, что и $B_{wn_k}, B_{wn_{kp}}$, а $u1_{kD'_w}(t)$ определяется выражениями, аналогичными (13), (14) с заменой $\dot{L}_k[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]$ на $\dot{L}_{k1}[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]$. В алгоритме (12) функция неопределенности $\dot{\Psi}_{D'}[f_0(\vec{\vartheta}-\vec{\vartheta}_2)]$ – обычная (в отличие от заданной формулой (10) функции сверхширокополосной системы).

В алгоритме (15) можно ограничиться формированием правой части, что позволит получить оценку яркости с разрешением, определяемым ядром $\left|\dot{\Psi}_{D'}[f_0(\vec{\vartheta}-\vec{\vartheta}_2)]\right|^2$. Однако можно и продолжить задачу извлечения функции $B_{ok}[f_0,\vec{\vartheta}_2,\vec{\lambda}(\vec{\vartheta}_2)]$ из-под знака интеграла известными методами решения некоррекных обратных задач [10, 11]. Деление в (15) на функцию $|\dot{F}_A(\vec{\vartheta}-\vec{\vartheta}_0,f)|^2$ практически является корректным, т. к. будучи диаграммой направленности элементарного излучателя в антенной решетке, эта функция широкая и обычно содержит все исследуемое изображение в пределах своего главного лепестка, где практически отсутствуют ее нулевые значения.

Основная последовательность операций, определяющая алгоритмическую структуру квазиоптимальной радиометрической системы, включает в себя задержку колебаний в различных точках раскрыва в соответствии с наклоном фронта падающего поля, обеспечивающую их синфазность для каждого направления $\vec{\vartheta}$; суммирование; декорреляцию; формирование сигналов, пропорциональных средней мощности декоррелированных колебаний; решение системы нелинейных уравнений (15) или без извлечения из-под знака интеграла искомых функций, или как интегральных уравнений с соответствующими их обращениями.

Внешне структурная схема радиометрической системы, соответствующая алгоритму (15), мало чем отличается от схемы, показанной на рис. 1. В ней необходимо заменить фильтры $\dot{L}_k[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]$ на фильтры $\dot{L}_{k1}[j2\pi f,\vec{\vartheta}_1,\vec{\lambda}_0]$ и блоки $|\dot{L}_{k1}(\vec{\vartheta})|^2$ на блоки $|\dot{F}_A(\vec{\vartheta}_1-\vec{\vartheta}_0,f)|^2$.

Выводы

Синтезирован оптимальный по критерию максимума правдоподобия алгоритм оценки распределения радияркости по угловым координатам в многоканальных пространственно-распределенных радиометрических системах. Основной операцией является формирование V_F-периодограммы, которая заключается в фильтрации принимаемых процессов по временным частотам f, фазовой задержке каждой частотной составляющей на величину $2\pi f\vec{\vartheta}\vec{r}'/c$ и синфазном суммировании задержанных сигналов по всем элементам антенной решетки.

Введен ряд допущений и разработаны структурные схемы пространственно-распредленных радиометрических систем при широкополосной и узкополосной обработке сигналов. В отличие от существующих схем, предложена операция декорреляции принятых колебаний в инверсном фильтре, увеличивающая число некоррелировнных отсчетов при оценке радияркости исследуемых объектов и повышающая точность этой оценки.

Список литературы: 1. *Караваев, В. В.* Основы теории синтезированных антенн / В. В. Караваев, В. В. Сазонов. – М. : Сов. радио, 1974. – 168 с. 2. *Томпсон, А. Р.* Интерферометрия и синтез в радиоастрономии : монография / А. Р. Томпсон, Д. М. Моран, Д. У. Свенсон ; пер. с англ. под ред. А. И. Матвеенко. – 2-е изд., перераб. и доп. – М. : Физматлит, 2003. – 624 с. 3. *Есепкина, Н. А.* Радиотелескопы и радиометры / Н. А. Есепкина,

Д. В. Корольков, Ю. Н. Парийский. – М. : Наука, 1973. – 416 с. 4. *Христиансен, У.* Радиотелескопы / У. Христиансен, И. Хегбом ; пер. с англ. под ред. А. А. Пистолькорса. – М. : Мир, 1988. – 304 с. 5. *Уилсон, Т. Л.* Инструменты и методы радиоастрономии : монография / Т. Л. Уилсон, К. Рольфс, С. Хюттемейстер ; пер. с англ. под ред. С. А. Трушкина. – М. : Физматлит, 2013. − 568 с. 6. *Ван Схонвелд, К.* Построение изображений в астрономии по функциям когерентности / К. Ван Схонвелд ; пер. с англ. под ред. Л. Р. Когана, В. И. Костенко. − М. : Мир, 1982. – 318 с. 7. *Борн М*. Основы оптики / М. Борн, Э. Вольф ; пер. с англ. − М. : Наука. 1973. 720 с. 8. *Волосюк, В. К.* Статистическая теория радиотехнических систем дистанционного зондирования и радиолокации : монография / В. К. Волосюк, В. Ф. Кравченко ; под ред. В. Ф. Кравченко. – М. : Физматлит, 2008. – 704 с. 9. *Фалькович, С. Е.* Основы статистической теории радиотехнических систем : учеб. пособие / С. Е. Фалькович, П. Ю. Костенко. – Харьков : Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т», 2005. − 390 с. 10. *Василенко, Г. И.* Восстановление изображений / Г. И. Василенко, А. М. Тараторин. − М. : Радио и связь, 1986. − 304 с. 11. *Тихонов, А. Н.* Методы решения некорректных задач / А. Н. Тихонов, В. Я. Арсенин. − М. : Наука, 1986. − 285 с.

Национальный аэрокосмический университет
имени Н.Е. Жуковского «ХАИ»

Поступила в редколлегию 03.10.2017

УДК.621.382(024)

И.В. БАРЫШЕВ, д-р техн. наук, К.А. ЩЕРБИНА, канд. техн. наук,
Е.П. МСАЛЛАМ, канд. техн. наук, М.А. ВОНСОВИЧ, А.В. ОДОКИЕНКО

АНАЛИЗ ПО ПОКАЗАТЕЛЯМ КАЧЕСТВА РАБОТЫ СХЕМ УЗКОПОЛОСНОЙ ФИЛЬТРАЦИИ НЕПРЕРЫВНОГО ДОПЛЕРОВСКОГО СИГНАЛА

Введение

При оценке качества работы схем узкополосной фильтрации непрерывных сигналов обычно используют следующие показатели [1, 2]: точность и надежность работы в условиях помех, устойчивость, время регулирования, характер переходного процесса и др.

Применительно к решению задач узкополосной фильтрации непрерывного доплеровского сигнала [3, 4] наиболее важными показателями качества фильтрации являются динамическая точность и флуктуационная погрешность или помехоустойчивость слежения в условиях действия аддитивной помехи.

На сегодняшний день разработано и применяется на практике большое разнообразие методов и схем практической реализации узкополосных следящих фильтров, обеспечивающих в той или иной степени требуемые показатели качества помехоустойчивой доплеровской фильтрации [5 – 8].

В связи с этим представляет теоретический и практический интерес сравнение возможностей узкополосной фильтрации различных фильтрующих схем.

В работе решается задача сравнительного анализа показателей качества работы известных и широко применяемых на практике схем фазовой и частотной автоподстройки частоты управляемого генератора, с перспективными схемами комбинированного типа, построенными на основе схем фазовой автоподстройки частоты (ФАПЧ) [7, 8] и разработанной авторами схемы ФАПЧ-СГ, реализованной на синхронизированном управляемом генераторе (УГ) с принудительной перестройкой частоты [9, 10].

Цель статьи – разработка методики оценки основных показателей качества работы следящего узкополосного фильтра, реализованного на синхронизированном автогенераторе с принудительной перестройкой частоты, количественной оценке показателей и их сравнение с такими же показателями известных фильтрующих схем доплеровского сигнала.

Содержание исследований

Как известно из практики сравнительного анализа количественных показателей работы различных устройств, систем и комплексов, основой его достоверности является объективность.

В нашем случае основными составляющими такой объективности являются: выбор основных $M\left[n(t)\right]=0$ показателей качества, характеризующих возможности опорного устройства или системы по которым производится сравнение; использование корректных аналитических формул; максимально возможное число количественных параметров и характеристик опорного образца, которые подлежат сравнению с разработанной схемой, устройством и т.д.

По методике, изложенной в [13], рассмотрим оптимизацию алгоритмов приема и обработки сигналов применительно к однолучевой ДИС.

Пусть на интервале времени $\left[t_0,\, t\right]$ наблюдается реализация случайного процесса

$$\xi(t)=S(t,\vec{\mathrm{X}})+n(t)\,, \tag{1}$$

где $n(t)$ – широкополосная флуктуационная помеха, аппроксимируемая белым гауссовским шумом с нулевым средним и функцией корреляции $M\left[n(t_1)\cdot n(t_2)\right]=0,5N_0\delta\left|t_2-t_1\right|$, $N_0=const$, который считается известным; $\vec{\mathrm{X}}(t)$ – марковский случайный процесс (вектор состояний).

Полезный сигнал задается выражением [13]

$$S(t)=A(t)\cos\left[\omega_0(t)-\frac{2D_r(t)}{C}+\psi(t)\right], \tag{2}$$

где $A(t)$ и ω_0 – амплитуда и частота полезного сигнала; $D_r(t)$ – дальность до точки отражения сигнала по направлению луча ДИС; $\psi(t)$ – случайная фаза.

В качестве математической модели, характеризующей изменения $D_r(t)$, примем линейную динамическую модель позволяющую учитывать движение ЛА. Фазовые флуктуации полезного сигнала (2) описываются системой стохастических дифференциальных уравнений [13]:

$$\frac{d\psi}{dt}=(\omega-\omega_0)+\sqrt{\frac{N_\varphi}{2}}\cdot n_\varphi(t), \tag{3}$$

$$\frac{d\psi}{dt}=-\gamma_\omega(\omega-\omega_0)+\sqrt{2\gamma_\omega\sigma_\omega^2}\cdot n_\omega(t),$$

где $(\omega-\omega_0)$ – некомпенсированный доплеровский сдвиг частоты; γ_ω – параметр, характеризующий ширину спектра доплеровских частот; $n_\varphi(t)$, $n_\omega(t)$ – гауссовские белые шумы с нулевым математическим ожиданием и единичной интенсивностью; σ_ω^2 – дисперсия флуктуаций средней частоты отраженного сигнала; $N_\varphi=const$, $N_\omega=const$.

Таким образом, в рассматриваемой задаче вектор состояний $\vec{\mathrm{X}}(t)$ имеет вид

$$\vec{\mathrm{X}}^T=\left[x_1=D_r,\ x_2=W_r,\ x_3=a_r,\ x_4=\psi,\ x_5=(\omega-\omega_0)\right], \tag{4}$$

где W_r – радиальная скорость в направлении луча; a_r – случайная составляющая (процесс) радиального ускорения ЛА.

Вектор состояний $\vec{\mathrm{X}}(t)$, подлежащий оцениванию, удовлетворяет уравнению

$$\frac{d\vec{\mathrm{X}}}{dt}=\vec{F}_x\vec{\mathrm{X}}+\vec{G}_x\vec{\mathrm{N}}_x(t),\ \vec{\mathrm{X}}(t_0)=\vec{\mathrm{X}}_0, \tag{5}$$

где $\vec{\mathrm{N}}_x^T(t)=\left[0,\ 0,\ n_a(t),\ n_\varphi(t),\ n_\omega(t)\right]$; матрицы $\vec{F}_x=\left[f_{ij}\right]$ и $\vec{G}_x=\left[g_{ij}\right]$ размером (5×5).

Уравнение, определяющее алгоритм приема и обработки непрерывных сигналов, применительно к (3), (4) и (5) после соответствующих преобразований, выполненных в [1], приводится к виду

$$\frac{d\vec{\mathrm{X}}}{dt}=\vec{F}_x\vec{\mathrm{X}}^*+\vec{K}(t)\vec{F}_1(t,\vec{\mathrm{X}}^*),\ \vec{\mathrm{X}}^*(t_0)=\vec{\mathrm{X}}_0, \tag{6}$$

где $\vec{K}(t)=\left[k_{j\omega}\right]$ – ковариационная матрица апостериорных ошибок фильтрации размером (5×5) [13].

Структурная схема синтезированного оптимального устройства приема и обработки сигналов (2), реализующая алгоритмы (6), представлена на рис.1, где $K_i = 2AN_0^{-1}\left[K_0\overline{k_{i1}(t)} - \overline{k_{i4}(t)}\right]$ – коэффициенты передачи усилительных блоков.

Остальные обозначения имеют прежний смысл. Рассматриваемое устройство представляет собой нелинейный фильтр с одним входом. Основными его элементами являются блоки формирования оценочных значений компонент вектора состояний $\vec{\mathrm{X}}(t)$, система фазовой автоподстройки, вырабатывающая опорный сигнал и вычислительное устройство ВУ.

Выходным сигналом устройства является напряжение, пропорциональное одиночному значению радиальной составляющей земной скорости ЛА $W_r^*(t)$ по данному лучу.

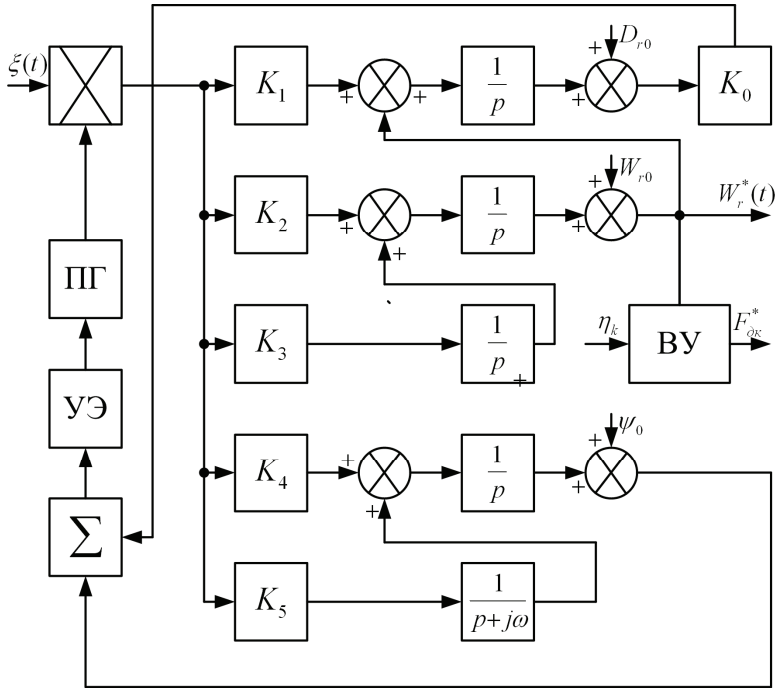


Рис. 1

Потенциальные характеристики точности и помехоустойчивости оптимального устройства приема и обработки сигналов (2) могут быть получены на основании решения уравнения вида [1]

$$\frac{d\vec{K}_H}{dt} = \vec{F}_H\vec{K}_H + \vec{K}_H\vec{F}^T + \vec{Q}_H + \vec{K}_H\vec{R}_H\vec{K}_H, \qquad (7)$$

где $\vec{K}_H$ – нормированная ковариационная матрица ошибок фильтрации с элементами $\delta_{ij} = \dfrac{\overline{k_{ij}(t)}}{(\sigma_i\sigma_j)}$; $i = \overline{1,5}$; $\vec{Q}_H = \left[\dfrac{q_{ii}^2}{\sigma_i^2}\right]$.

Матрицы $\vec{F}_H, \vec{Q}_H, \vec{R}_H$ имеют размер (5×5) и содержат отличные от нуля элементы: $f_{12} = \sigma_2\sigma_1^{-1}$; $f_{23} = \sigma_3\sigma_2^{-1}$; $f_{33} = -\alpha$; $f_{45} = \sigma_5\sigma_4^{-1}$; $f_{55} = -\gamma_\omega$; $g_{33} = 2a$; $g_{44} = \gamma_\omega D_\varphi\sigma_\varphi^{-2}$; $r_{44} = 2\gamma_\omega q\sigma_\varphi^{-2}$, где $q = A^2/(2\gamma_\omega N_0)$ – отношение сигнал/помеха в наблюдаемом процессе (реализации) $\xi_1(t)$; $D_\varphi = N_\varphi/(2\gamma\omega)$.

На рис. 2 и 3 приведены результаты расчетов погрешностей оценок скоростной W_r и частотной $(\omega-\omega_0)$ компонент вектора состояния $\vec{\mathrm{X}}^*(t)$, выполненных на ЭВМ для следую-

щих значений обобщенных параметров: $q = 1 \div 100$; $\gamma_\omega = 10^3$ с$^{-1}$; $a = 10^{-2}$ с$^{-1}$; $\sigma_1 = 50$ м; $\sigma_2 = 100$ мс$^{-1}$; $\sigma_3 = 10$ мс$^{-2}$; $\sigma_4 = \frac{\pi}{\sqrt{3}}$; $\sigma_\omega = 10$ Гц; $D_\varphi = 10^{-3}$. При расчетах было принято $\sigma_{ii}(0) = 1$, $\sigma_{ij}(0) = 0$.

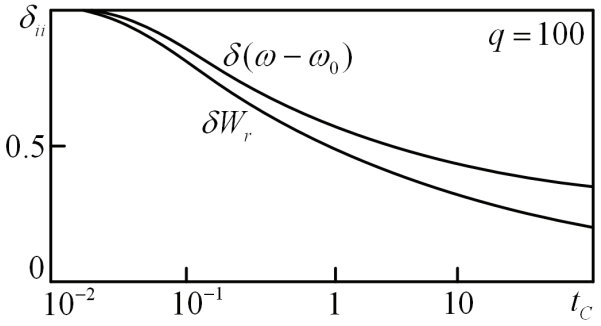


Рис. 2

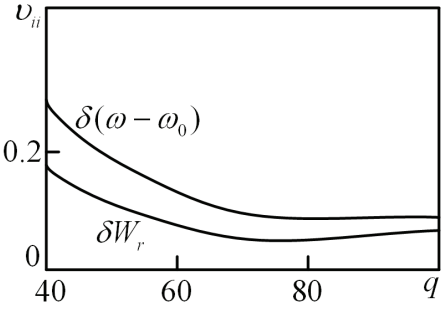


Рис. 3

Рассмотренная методика и схемная реализация оптимального устройства приема и обработки доплеровских сигналов ориентирована на аналитическое описание сигнала в виде узкополосного случайного процесса, в котором информационные параметры были представлены в виде непрерывного марковского процесса, описываемого системой стохастических уравнений (7). На самом деле доплеровский сигнал формируется участком протяженной поверхности, «освещаемой» источником излучения, расположенном на борту ЛА, и представляет собой колебание со сложной амплитудно-частотной модуляцией [2].

Не менее важной проблемой, возникающей при использовании оптимальной структуры, представленной на рис. 1, является разрешение противоречия между условиями достижения оптимальности, устойчивости и условием повышения динамической точности.

Исходя из изложенного для подтверждения достоверности и объективности выполнения процедуры сравнения необходимо использовать при сравнительном анализе количественные характеристики и параметры реально действующих устройств, выполняющих аналогичные с разработанным устройством функции. Поэтому была разработана табл. 1 показателей качества фильтрации нескольких типов СДФ, включающая шесть показателей качества и основные аналитические соотношения по которым они рассчитываются.

В качестве опорного устройства сравнения выбрана схема ФАПЧ 1-го порядка с RC фильтром с которым сравниваются комбинированная ФАПЧ 2-го порядка и разработанная схема ФАПЧ-СГ на основе синхронизированного УГ с принудительной перестройкой по частоте.

Источником реальных данных, необходимых для выполнения соответствующих расчетов по приведенным в табл. 1 формулам, стала схема СДФ на основе ЧАП с квадратурно-фазовым частотным дискриминатором, которая применяется в ДИСС-013 и ДИСС-016.

Приведем основные данные этих реальных узкополосных следящих измерителей скорости ЛА. $\Delta f_Э = 0,4...24$ кГц с переносом на среднюю частоту УГ $F_Г \simeq 500$ кГц; полоса доплеровских частот $0,8 \div 12$ кГц; погрешность измерения частоты $\sigma_{F_1} = 0,4\%$ на частотах $\geq 2,5$ кГц; на частотах $F_Д \geq 2,5$ кГц слежение включается при $\frac{P_C}{P_Ш} = 10$ дБ; на частотах ниже $2,5$ кГц слежение включается при $\frac{P_C}{P_Ш} = 8$ дБ; время поиска не более 15 с; постоянная времени RC фильтра $T_{RC} = 0,1...1$ с; коэффициент шума первых смесителей резонансного тракта ДИСС не более 12 дБ, а УПЧ – $2,5$ дБ; чувствительность приемно-усилительного тракта ≥ 110 дБ/мВт; постоянная времени АРУ $0,32$ с.

Используя приведенные реальные параметры, рассчитаем величину коэффициента усиления K схемы ФАПЧ 1-го порядка при следующих данных: $F_{Д_{СР}} = 5$ кГц; $\sigma_{F_Д} = 0{,}1\%$; $T_{RC} = 0{,}1$ с; $\Delta f_Э = 15$ кГц; $q^2 = 1$. Тогда получим следующие результаты

$$\sigma_\omega^2 = 4\pi^2\sigma_F^2 = 4\pi^2 \cdot 5^2 = 985{,}96 \text{ рад}^2/\text{с}^2;$$

$$K^2 = \sigma_\omega^2 \cdot 4\pi \cdot \Delta f_Э \cdot T_{RC} = 985{,}96 \cdot 4 \cdot 3{,}14 \cdot 15000 \cdot 0{,}1 = 18575486{,}4;$$

$$K = 18575486{,}4^{\frac{1}{2}} = 4309 \text{ рад/с}.$$

Положим $K \simeq K_y = \dfrac{E_Г}{E_0} \simeq 4500$ и определим $\omega_0 = 2\pi f_0$ – среднюю частоту синхронизированного УГ разработанного СДФ

$$f_{0F} = \sqrt{\sigma_F^2 K_y^2 / \left[1 - \frac{\pi}{4}\right]} = \sqrt{25 \cdot 4309^2 / 0{,}215} \simeq 46465 \text{ Гц}.$$

Увеличим f_0 до $f_0 = 100\,000$ кГц и пересчитаем K_y без изменения σ_ω^2. Тогда $K_y = 10\,000$.

Из приведенных расчетов видно, что при заданных параметрах опорной схемы: $K = 4309$ рад/с; $\Delta f_Э = 15\,000$ кГц; $T_{RC} = 0{,}1$ с; $\sigma_F = 0{,}1\% F_{CP}$ или $\sigma_F = 5$ Гц и заданных параметрах разработанной схемы СДФ: $K = 9500$; $f_0 = 100\,000$ Гц и одинаковых значениях q^2 для обеих схем, выигрыш в флуктуационной частотной погрешности $k_\omega = \dfrac{\sigma_{ФАПЧ}^2}{\sigma_P^2} = \dfrac{985{,}96}{860} = 1{,}5$, σ_P^2 – дисперсия разработанного варианта.

Расчет выигрыша по флуктуационной погрешности фазы дает следующий результат. Рассчитаем коэффициент при $\dfrac{\pi\omega_0}{K \cdot \Delta f_Э} = \dfrac{2\pi^3 \cdot 10^5}{9500 \cdot 15000} \simeq 0{,}04$; $k_\varphi = \dfrac{1}{0.04} = 25$. Здесь проведено сравнение коэффициентов: 1 рад^2 – для ФАПЧ 1-го порядка с рассчитанным $\sigma_{\varphi_P}^2$ – для синхронизированного УГ.

Выигрыш по полосе захвата определим следующим образом. Вначале рассчитаем величину $\gamma_З$

$$\gamma_З = \frac{1{,}2}{\sqrt{0{,}1 \cdot 15000}} = 0{,}03.$$

Тогда абсолютная полоса захвата $\Delta F_З = 0{,}03\Delta f_Э = 450$ Гц и выигрыш составит

$$k_З = \frac{1500}{450} = 33{,}3.$$

Рассчитаем выигрыш во времени установления переходного процесса задав для ФАПЧ величину $\gamma_H = 0{,}5$. Тогда

$$\tau_{ФАПЧ} = \frac{2}{1500\sqrt{1-0{,}5}} \ln 114\sqrt{1-0{,}5} = 0{,}82 \cdot 10^{-3}\,\mu S;$$

Таблица 1

Показатели качества фильтрации

	Тип СДФ / Показатели качества фильтрации	Динамическая погрешность		Флуктуационная погрешность		Полоса захвата	Время установления переходного процесса $\tau_{УСТ}$
		$\varphi = \alpha_1 t$	$\varphi = \alpha_2 t^2 / 2$	σ_ω^2	σ_φ^2		
		$\theta_{1УСТ}(t)$	$\theta_{2УСТ}(t)$				
1	ФАПЧ 1-го порядка с RC фильтром	$\frac{\alpha_1}{K}$	–	$\frac{K^2}{4\pi\Delta f_Э T_{RC}}\left(\frac{1}{q^2}\right)$	$\frac{1}{q^2}$	$\gamma_З = \frac{1,2}{\sqrt{T\Delta f_Э}}$	$\frac{2}{\Delta f_Э\sqrt{1-\gamma_H}}\ln 114\sqrt{1-\gamma_H^2}$
2	Комбинированная ФАПЧ 2-го порядка	..	$\frac{2(T_{ЧД}+T_Г)}{K}$	$\frac{\omega_0^2}{K^2}\left[1-\frac{\pi}{4}\right]\left(\frac{1}{q^2}\right)$	$\frac{\pi\omega_0}{K\Delta f_Э}\left(\frac{1}{q^2}\right)$	$\Delta f_Э$	$\le \frac{1}{\Delta f_Э}$
3	ЧАП с квадратурно-фазовым частотным дискриминатором	–	–	$K_F^2\Delta f_Э \Delta F_Ф\left(\frac{1}{q^2}\right)$	–	$\Delta f_Э$ схема поиска, захвата и слежения	Время поиска $T_П$ не более 15 с
4	Схема ФАПЧ-СГ	0	$\frac{2\tau_Г\cdot\alpha_2}{K_y}$	$\frac{\omega_0^2}{K_y^2}\left[1-\frac{\pi}{4}\right]\left(\frac{1}{q^2}\right)$	$\frac{\pi\omega_0}{K_y\Delta f_Э}\left(\frac{1}{q^2}\right)$	$\Delta f_Э$	$\le \frac{1}{\Delta f_Э}$

Здесь $\alpha_1 t$ – линейное изменение фазы; $\alpha_2 t^2/2$ – квадратурное изменение фазы; $K = \frac{1}{2}k_Д E_0 S_y$ – коэффициент усиления контура ФАПЧ; $K_y = E_Г / E_0$; $K_F < 1$ – коэффициент, учитывающий частотную характеристику следящей системы; $\Delta f_Э \ge \left|F_{Д\max} - F_{Д\min}\right|$ – полоса пропускания линейного тракта усиления ДИС; $\Delta f_Э \simeq \Delta_{СН}$; $\tau^*_{УСТ}$ – приведена в [13]; σ_ω^2 для ЧАП с квадратурно-фазовым дискриминатором заимствована из [13]; γ_H – относительная начальная расстройка $\gamma_H = \Delta_H / \Delta_{СН}$.

$$\tau_P = \frac{1}{15000} = 0,66\mu S .$$

Выигрыш во времени установления составит

$$k_\tau = \frac{\tau_{ФАПЧ}}{\tau_p} = 1,242 .$$

Результаты выполненных расчетов сведены в табл. 2.

Таблица 2

Результаты выполненных расчетов

k_i, $i = 1 \div 6$	$k_{\theta_{1УСТ}}(t)$	$k_{\theta_{2УСТ}}(t)$	k_ω	k_φ	$k_З$	k_τ
Числовая величина	$>>1$	–	1,5	25	33	1,242

Расчет минимальной дисперсии флуктуационной погрешности схемы ЧАП с квадратурно-фазовым частотным дискриминатором можно выполнить по заданной величине относительной величины СКО $\sigma_F = 0,1\%$ от $F_{Д_{СР}} = 5$ кГц.

Тогда $\sigma_F^2 = 25$ Гц^2, или $\sigma_\omega^2 = 4\pi^2 \cdot 25$ Гц$= 985,96$ рад^2.

Полученный результат совпадает с дисперсией частотной ошибки для ФАПЧ 1-го порядка. Следовательно выигрыш по величине частотной флуктуационной ошибки разработанной схемы ФАПЧ-СГ будет равен 2.

Расчет выигрыша по динамической погрешности $\theta_{2УСТ}(t)$ разработанной схемы с комбинированной ФАПЧ 2-го порядка выполнен по формуле $k_{\theta_2}(t) = \frac{2(T_{ЧД} + T_\Г)}{2\tau_\Г} = 2$, при $\tau_\Г = T_\Г = T_{ЧД}$.

Средний суммарный показатель качества схемы ФАПЧ-СГ, реализованной на синхронизированном УГ с принудительной перестройкой частоты с исключением больших величин $k_{\theta_{2УСТ}}(t)$, k_φ и $k_З$ при одинаковом весе всех остальных показателей, равном 1, будет порядка $1,5$ (с учетом ЧАП и ФАПЧ 2-го порядка)

$$\text{П}K_\Sigma = \frac{1}{4}\sum_4 = \frac{1}{4}(k_\omega + k_\tau + k_{\theta_2(t)} + k_{\omega_{ЧАП}}) \simeq 1,5 .$$

Обратим внимание на важное обстоятельство.

Разработанная и исследованная схема ФАПЧ-СГ обеспечивает достижение конкретных величин выигрыша по всем выбранным для оценки среднего суммарного выигрыша показателям.

Если такую же процедуру применить, например, для СДФ реализованного на ФАПЧ 1-го порядка, то средний суммарный показатель качества окажется существенно меньше единицы, поскольку такой узкополосный фильтр обладает только одним высокоэффективным показателем, а именно – минимумом дисперсии флуктуаций фазы $\sigma_\varphi^2 \geq \frac{1}{q^2}$. Остальные показатели качества узкополосного фильтра реализованного на ФАПЧ 1-го порядка будут хуже чем у разработанного фильтра. Это можно увидеть проанализировав остальные показатели качества по табл. 1.

Заключение

Разработана методика оценки показателей качества работы следящей схемы фильтрации, реализованной на синхронизированном генераторе с принудительной перестройкой частоты. При этом получены простые расчетные формулы (см. табл. 1) оценок показателей качества работы данной схемы.

Выполнен сравнительный анализ показателей качества следящих схем узкополосной фильтрации, реализованных на схемах ФАПЧ 1-го порядка, ФАПЧ 2-го порядка и ФАПЧ-СГ с принудительной перестройкой частоты. При этом суммарный средний показатель качества схемы на синхронизированном генераторе выше в 1,5 раза, а по отдельным показателям – в десятки раз, аналогичных показателей, рассчитанных для схем ФАПЧ и ЧАП.

Список литературы: 1. *Фомин, А.Ф., Хорошавин, А.И., Шелухин, О.И.* Аналоговые и цифровые синхронно-фазовые измерители и демодуляторы. – М. : Радио и связь, 1987. 2. *Шелухин, О.И.* Радиосистемы ближнего действия. – М. : Радио и связь, 1989. 3. *Островитян, Р.В., Басалов, Ф.А.* Статистическая теория радиолокации протяженных целей. – М. : Радио и связь, 1982. 4. *Штагер, Е.А.* Рассеяние радиоволн на телах сложной формы. – М : Радио и связи, 1986. 5. *Стеклов, В.К., Руденко, А.А., Юдин, В.К.* Комбинированные системы ФАП. – К. : Техника, 2004. 6. *Шахгильдян, В.В., Ляховский, А.А*. Системы фазовый синхронизации с элементами дискретизации. – М. : Радио и связь, 1989. 7. *Volosyuk, V. K., Zhyla, S. S., Antonov, M. O. and Khaleev, O. A.* Optimal acquisition mode and signal processing algorithm in syntetic aperture radar // 2017 IEEE 37th International Conference on Electronics and Nanotechnology (ELNANO). – Kiev, 2017. – P. 511-516. 8. *Pavlikov, V., Volosyuk, Zhyla, S., Van, H. N. and Van, K. N.* A new method of multi-frequency active aperture synthesis for imaging of SAR blind zone under aerospace vehicle // 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). – Lviv, 2017. – P. 118-120. 9. *Зайцев, Г.Ф., Стеклов, В.К.* Комбинированные следящие системы. – К. : Техника, 1978. 10. *Зайцев, Г.Ф., Стеклов, В.К.* Радиотехнические системы автоматического управления высокой точности. – К. : Техника, 1988. 11. *Вонсович, М.А.* Структурный синтез комбинированной системы частотно-фазовой автоподстройки частоты, совмещенной с фильтрующей схемой спектра входного сигнала / М.А. Вонсович, К.А. Щербина, В.В. Печенин, Е.П. Мсаллам // Системи управління, навігації та зв'язку. – 2015. – №4(36). – С. 38-43. 12. *Шахгильдян, В.В., Ляховский, А.А.* Системы фазовой автоподстройки частоты. – М. : Связь, 1972. 13. *Ярлыков, М.С.* Применение марковской теории нелинейной фильтрации в радиотехнике / М.С. Ярлыков. – М. : Сов. радио, 1980. – 360 с.

Национальный аэрокосмический университет
имени Н. Е. Жуковского«ХАИ»,
Филиал «Дельта-лоцман» ГП «АМПУ»
Министерства инфраструктуры Украины

Поступила в редколлегию 08.11.2017

УДК 621. 396. 962

В.Є. КУДРЯШОВ, канд. техн. наук, С.М. ТАМАШ, Д.С. ШМАКОВ

РОЗНЕСЕНА ДВОХПОЗИЦІЙНА РАДІОМЕТРИЧНА СИСТЕМА КАРТОГРАФУВАННЯ ОБЄКТІВ

Постановка проблеми

Рознесена радіометрична система (РМС) [6, 7, 9, 13] дозволяє вимірювати кутові координати, різницю ходу та швидкість об'єктів. Картографування земних та космічних об'єктів потребує визначення дальності дії РМС [1 – 4, 11, 12]. У теперішній час відсутній вираз для розрахунку вказаної дальності дії при картографуванні. Задача обґрунтування варіантів рівнянь дальності картографування рознесеної двохпозиційною РМС є важливою та актуальною. При цьому требо врахувати і заважаючі сигнали, які є на розкриві антен кореляційного радіометра, а також розширення смуг пропускання РМС для підвищення енергетичних характеристик та розрізнювальної здатності за різницею ходу.

Аналіз публікацій, які представлені у [1 – 5,7 – 12, 22], не дає можливості визначити дальність дії рознесеної двохпозиційної РМС при картографуванні земних та космічних об'єктів. Лише у публікаціях [6, 12] розглядається виявлення повітряних та наземних цілей без врахування коливань, що заважають, які знаходяться на розкриві антен рознесеної РМС. В статтях [4, 5, 7 – 12] є структурні схеми РМС, результати їх експериментальних досліджень та обробки радіометричних зображень.

Мета статті – обґрунтування варіантів рівнянь дальності дії радіотеплолокаційного спостереження рознесеної двохпозиційною РМС картографування земних та космічних об'єктів, варіантів підвищення розрізнювальних здатностей за різницею ходу та відносною швидкістю об'єктів.

Виклад основного матеріалу

Загальна схема побудови бортової РМС наведена на рис. 1. Літак рухається над поверхнею з швидкістю $\vec{V}$, на ньому знаходяться два просторово рознесені пункти прийому П1, П2 кореляційного радіометра. Відстань між П1, П2 є базою рознесеної системи і позначена на рис. 1 через Б. За час зйомки одної строки поверхні літак її пролітає. Таким чином будується радіометричне зображення. Збільшення вхідної смуги пропускання системи та (або) величини Б збільшує розрізнювальну здатність (РЗ) за різницею хода у кожному положенні антен, тобто зменшує розмір пікселя зображення.

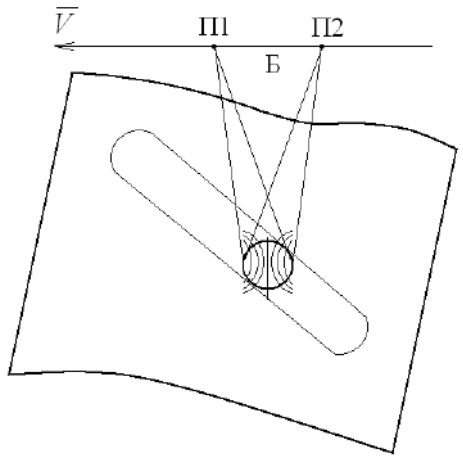


Рис. 1. Загальна схема побудови бортової РМС картографування земної поверхні

Основним елементом рознесеної двохпозиційної РМС [1 – 3, 10, 16, 22] є кореляційний радіометр. Чутливість кореляційного радіометра [16]:

$$\Delta T_{\min} = \frac{\alpha\left(T_{\text{пр}} + T_{\text{а}}\right)}{\sqrt{\Pi_{\text{вх}} / \Pi_{\text{вих}}}}, \qquad (1)$$

де α – const кореляційного радіометра ($\sqrt{2}$); $T_{\text{пр}}$, $T_{\text{а}}$ – відповідно температури радіоприймача та антени радіометра; $\Pi_{\text{вх}}, \Pi_{\text{вих}}$ – вхідна та вихідна смуги пропускання радіометра.

Широкосмуговий кореляційний радіометр. На основі створених приладів [15] можливо збільшення $\Pi_{\text{вх}}$, наприклад у шість разів, при переході з 8 до 3 мм діапазону довжин хвиль [19]. Вказане надає зниження $\Delta T_{\min}$, що важливо при картографуванні малорозмірних

об’єктів (МО). Розширення $П_{вх}$ узгоджується з регламентом радіозв’язку [19]. Так, при переході з 8 до 3 мм діапазону РЗ за різницею хода по лінії бази підвищується з 0,3 до 0,05 м. Освоєння промисловістю елементної бази більше 275 ГГц дозволить застосовувати $П_{вх} > 40$ ГГц, що відповідає РЗ за різницею хода по лінії бази $< 10^{-2}$ м.

Даний підхід може розглядатися і для інфрачервоного діапазону (ІЧ) довжин хвиль. Так, у вікні прозорості атмосфери 3,3 – 4,2 мкм реалізується РЗ за різницею хода по лінії бази 15,4 мкм, що суттєво підвищить якість зображень. Хоча при цьому постає складна науково-технічна задача створення лінії затримки з багатьма відводами та вибір детекторів.

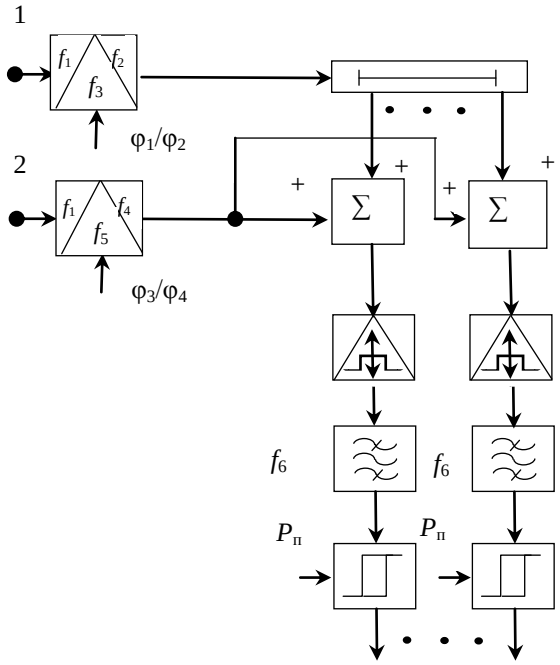


Рис. 2. Схема широкосмугового кореляційного радіометра

У теперішній час неможливо реалізувати перемножувач радіометра з $П_{вх}$ 6 ГГц. Один з варіантів побудови приладу з необхідною $П_{вх}$ приведена на рис. 2. На вході встановлено модулятори, які забезпечують «фарбування» сигналів за фазою φ_i з частотами f_3 та f_5. Якщо f_3, f_5 дорівнюють наприклад 1,1 та 1,9 кГц, то взаємна кореляційна функція (ВКФ) корисних сигналів фільтрується на частоті f_6 у 3 кГц. Лінія затримки має відведення через 0,5 ВКФ.

В подальшому (рис. 2) проводиться складання сигналів першого та другого каналів прийому у суматорах (∑). Квадратичне детектування на квадраторах та фільтрація на f_6 надає значення ВКФ. Коливання вихідних фільтрів інтеграторів радіометра порівнюються з рівнем порогів $P_п$. Значення $P_п$ визначає рівень помилкової тривоги F при картографуванні різноманітних поверхонь.

При створенні системи в ІЧ діапазоні довжин хвиль можливо застосовувати загальну структурну схему приладу, рис. 2.

Температури, тілісні кути та втрати по трасі поширення. За виразом (1) знаходимо з рівняння [18]:

$$T_{пр} = T_0 (K_ш - 1), \tag{2}$$

де $К_ш$ – коефіцієнт шуму радіоприймального пристрою радіометра; T_0 – температура середовища, яке оточує кореляційний радіометр.

Температура (1) для кожного з двох каналів прийому при картографуванні поверхонь [6, 13]:

$$T_а = (1-\beta)\eta \left[T_{атм} + T_з (1-\delta) + \sum_{i=1}^{n} t_i \delta_i + T\delta \right] + \beta\eta \left(T_{атм} + T_з + \sum_{j=1}^{k} t_j \delta_j \right) + (1-\eta) T_0. \tag{3}$$

Перша складова (3) надає антенну температуру прийняту у тілесному куті головної пелюстки діаграми спрямованості (ДС) антени радіометра $\Omega_{гл}$. Друга складова – зовні $\Omega_{гл}$, а третя складова характеризує особисті шуми антен радіометра. Причому: β – коефіцієнт враховує частку ненаправленого випромінювання, яке приймається антеною зовні $\Omega_{гл}$;

η – коефіцієнти корисної дії антен; $T_{\text{атм}}, T_{\text{з}}, T$ – відповідно шумові (радіояскраві) температури атмосфери, землі та МО картографування; t_i, t_j – відповідно шумові температури поверхонь, що заважають прийому корисних сигналів, які знаходяться у головній та бокових пелюстках ДС антен; $i = 1,2\ldots n$ та $j = 1,2\ldots k$;

$$\delta = \Omega_{\text{мо}} / \Omega_{\text{гл}}, \tag{4}$$

де $\Omega_{\text{мо}}$ – тілесний кут зайнятий МО [1,13]; δ_i, δ_j – теж саме що і δ, але для сигналів, які заважають прийому коливань МО, причому:

$$\Omega_{\text{оп}} = S / R^2, \quad \Omega_{\text{гл}} = 4\pi\eta / G, \tag{5}$$

де S – площина МО; R – дальність до нього; G – коефіцієнти підсилювання антен [17,20]

$$G = \left(3{,}2 \cdot 10^4 L_1 L_2\right) \Big/ \left[\lambda\left(180/\pi\right)\right]^2, \tag{6}$$

де L_1, L_2 – розміри антен у горизонтальній та вертикальній площинах відповідно; λ – центральна довжина хвилі РМС.

Якщо однакових розмірів антен у системі L_i з виразів (4), (5) отримуємо:

$$\delta = \left(SG\right) \Big/ \left(4\pi\eta R^2\right). \tag{7}$$

Температура атмосферного випромінювання, яка спостерігається при зенітному куті ϕ [1, 13, 16]:

$$T_{\text{атм}}(\phi) = \left(T_0 - 30\right)\left[1 - L(\phi)^{-1}\right], \tag{8}$$

де $L(\phi)$ – повне поглинання (загасання) в атмосфері (сумарні втрати по трасі поширення радіометричних (РМ) сигналів).

При використання моделі [1, 16] і середніх відстаней R $(<8\text{км})$ вираз для сумарних втрат по трасі поширення має вигляд

$$L(\phi) \approx \exp\left[0{,}23 B R \left(\cos\phi\right)^{-1}\right], \tag{9}$$

де B – коефіцієнт поглинання РМ сигналів при наявності в атмосфері кисню, пари води, пилу.

У виразах (8) та (9) використовується модель плоскої поверхні картографування, яка покрита однорідним шаром атмосфери. Для визначення коефіцієнтів В використовуємо підходи, які приведені у [1, 14]. При ясній погоді враховано лише поглинання кисню і водяних парів у стандартних умовах. Щільність водяних парів, при цьому, дорівнює 7,5 $\text{гр}/\text{м}^3$. Також визначені значення В при дощу середньої сили – 4 мм/годину. Значення коефіцієнтів В для довжини хвилі ~3,4 мм, коли ясно та дощ середньої сили відповідно дорівнюють 1,0442 і 1,9444 разів/км. Результати розрахунку за виразом (9), при зміні R від 1,5 до 5,5 км приведені на рис. 3. Криві $T_{\text{атм}}1(\phi)$ та $T_{\text{атм}}2(\phi)$ відповідно відображають значення температур атмосфери якщо ясно, або дощ. Перша крива $T_{\text{атм}}1(\phi, 1.5)$ безперервна та друга $T_{\text{атм}}2(\phi, 1.5)$ (позначена точками) надають значення температур, коли R дорівнює 1,5 км. Криві $T_{\text{атм}}1(\phi, 3.5)$ (тире) та $T_{\text{атм}}2(\phi, 3.5)$ (точки тире) побудовані при R у 3,5 км. На рис. 3 п'ята ($\times\times\times$) і шоста ($\circ\circ\circ$) криві здобуті коли R – 5,5 км.

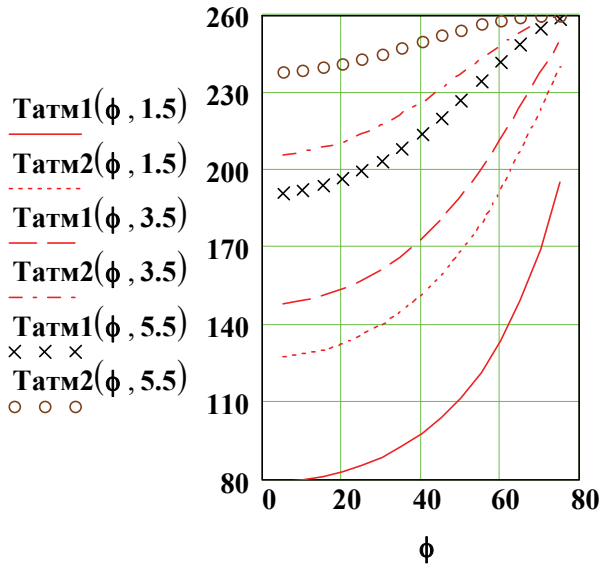


Рис. 3. Температура атмосферного випромінювання $T_{\text{атм}\,i}(\phi)$, яка спостерігається при зенітному куті ϕ та зміні дальності R від 1,5 до 5,5 км

Температура $T_{\text{з}}$ обрана на основі експериментальних даних радіояскравих температур [16] для сухого піску (гравію) ~ 252 *K*. При цьому $\phi \le 30^\circ$.

Радіояскрава температура МО T залежить від її випромінювальної здатності χ, кута ϕ та термодинамічної температури $T_{\text{т}}$, так $T(\phi) = \chi(\phi) T_{\text{т}}$ [1, 16]. Для шершавих поверхонь значення $\chi\left(\phi \le 30^\circ\right)$ змінюється у межах від ~0,91 до ~0,88, для гладкого вологого ґрунту ~0,67. При знаходженні автомобіля на однорідній поверхні [16], коли $\chi\left(\phi \le 30^\circ\right)$ дорівнює ~0,72 [13].

Для виявлення МО гладкого вологого ґрунту приймаємо T у 194 *K*.

Радіояскраві випромінювання завад T_{ϕ} (фону, що корельований та власних шумів приймальних каналів) при відсутності сигналу МО на вході системи визначається виразом

$$T_{\phi} = (1-\beta)\eta\left[T_{\text{атм}} + T_{\text{з}}(1-\delta) + \sum_{i=1}^{n} t_i \delta_i\right] + \beta\eta\left(T_{\text{атм}} + T_{\text{з}} + \sum_{j=1}^{k} t_j \delta_j\right) + (1-\eta) T_0. \quad (10)$$

Відношення сигнал-завада та дальність дії системи. Якщо у РМС однакові антени та канали прийому то відношення сигнал-завада γ_i $(i = 1, 2)$ у кожному з каналів дорівнює [14, 13]:

$$\gamma_i = P_{\text{с}i} \big/ P_{\phi i} = \left(P_{\text{а}i} - P_{\phi i}\right) \big/ P_{\phi i}, \quad (11)$$

де $P_{\text{а}i}, P_{\phi i}$ – відповідно потужність сигналів на вході РМС при наявності та відсутності сигналу від МО, так [18, 23]:

$$\begin{aligned} P_{\text{а}i} &= k T_0 \Pi_{\text{вх}} \left(K_{\text{ш}} - 1 + \frac{T_{\text{а}i}}{T_0}\right) \\ P_{\phi i} &= k T_0 \Pi_{\text{вх}} \left(K_{\text{ш}} - 1 + \frac{T_{\phi i}}{T_0}\right) \end{aligned}, \quad (12)$$

де k – постійна Больцмана.

Якщо технічні параметри $(T_0, K_{\text{ш}}, \beta, \eta, G\ldots)$ кожного з каналів однакові та провівши ряд математичних перетворень з формул (2) – (7), (10) – (12) здобули γ для одного з каналу прийому РМС:

$$\gamma = \frac{(1-\beta) S G \left|T - T_{\text{з}}\right|}{4\pi\alpha R^2 L\left[T_0\left(K_{\text{ш}} - \eta\right) + A\right]}, \quad (13)$$

де $L-$ втрати в РМС та

$$A=\eta\left[T_{\text{атм}}+T_{\text{з}}+(1-\beta)\sum_{i=1}^{n}t_i\,\delta_i+\beta\sum_{j=1}^{k}t_j\delta_j\right]. \tag{14}$$

Після кореляційного стискання, тобто оцінювання ВКФ в РМС, відношення сигнал-шум ν на виході системи визначається з виразу [14, 6, 13]:

$$\nu=\frac{\Pi_{\text{вх}}\tau_{\text{н}}\rho^2}{1+\rho^2}, \tag{15}$$

де $\tau_{\text{н}}$ – час накопичення у кореляційному радіометрі; $\rho-$коефіцієнт кореляції вхідних коливань, при $\gamma_1=\gamma_2$

$$\rho=\gamma/(1+\gamma). \tag{16}$$

Якщо $\nu=5{,}64$ рази (15) то імовірність вірного виявлення МО на поверхні картографування $P_{\text{в}}$ дорівнює 0,5 при фіксованому рівні помилкової тривоги $F-10^{-2}$ [14,6]:

$$P_{\text{в}}=F^{(1+\nu)^{-1}}.$$

Використовуємо вирази (15) та (16), при умові що дальність до МО суттєво більше відстані між антенами кореляційного радіометра Б (рис. 1), γ визначаємо з рівняння:

$$\gamma=\left[\nu+\sqrt{\nu(K_{\text{ст}}-\nu)}\right]\Big/(K_{\text{ст}}-2\nu), \tag{17}$$

де $K_{\text{ст}}-$коефіцієнт кореляційного стискання, причому $K_{\text{ст}}=\Pi_{\text{вх}}\tau_{\text{н}}$.

Враховуючи (17) з виразу (13) отримали рівняння дальності дії рознесеної двохпозиційної РМС:

$$R=\sqrt{\frac{|T-T_{\text{з}}|SG(1-\beta)}{4\pi\alpha\gamma L\left[T_0(K_{\text{ш}}-\eta)+A\right]}}, \tag{18}$$

Відношення сигнал-шум на виході RC інтегратора [21] дорівнює:

$$\nu=\frac{1}{2}\left(\frac{m}{\sigma}\right)^2=\frac{1}{2}\left[\frac{1-\exp(-\Pi_{\text{вих}}t/3)}{\sqrt{1-\exp(-2\Pi_{\text{вих}}t/3)}}\right]^2, \tag{19}$$

де $m,\sigma-$відповідно середнє значення та середньоквадратичне відхилення на виході інтегратора; $t-$ час інтегрування кореляційного радіометра.

Для забезпечення найбільшої смуги картографування (строчка, яка перпендикулярна $\vec{V}$ на рис. 1) обмежили значення $\tau_{\text{н}}$ (15) на рівні $\tau_{\text{н}}=3/\Pi_{\text{вих}}$. При цьому $m\neq1$ (19) та втрати у величині ν дорівнюють $(1/0{,}9514)^2\approx1{,}105$ рази. Тоді отримуємо $\nu=5{,}64\cdot1{,}105\approx6{,}23$ рази.

На рис. 4 представлені результати розрахунку за виразом (18) при наступних типових технічних характеристиках [13, 15 – 18]: $T=194K$; $T_{\text{з}}=252K$; $T_{\text{атм}}=209\,K$; $T_0=290\,K$; $\beta=0{,}31$; $L=2$; $K_{\text{ш}}=2{,}7$; $\eta=0{,}78$; $\lambda=3{,}4\cdot10^{-3}$м; $L_1=L_2=90\lambda$; $\Pi_{\text{вх}}=6\cdot10^9$ ГГц; $\Pi_{\text{вих}}=310$ Гц; $\nu=6{,}23$; $F=10^{-2}$; $P_{\text{в}}=0{,}5$; $t_i\approx t_j\approx0$, тобто картографування ведеться на

протяжній однорідній поверхні; S – змінюється в межах від 2 до 10^3 м^2; значення $T_з$ це радіояскрава температурі піску (або гравію), коли $\phi < 30^\circ$.

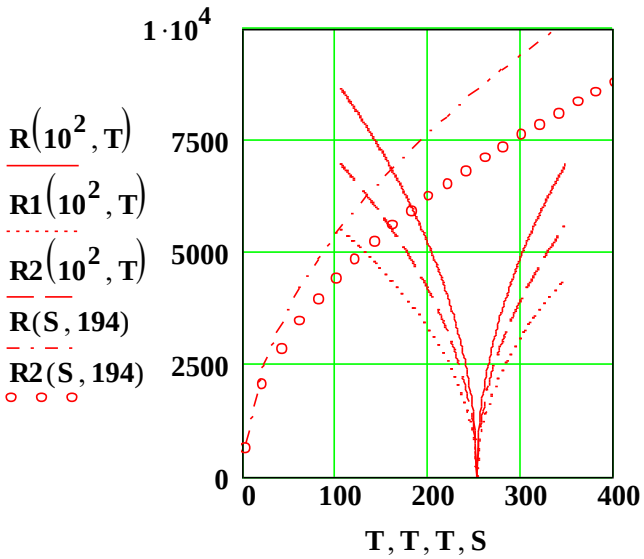


Рис. 4. Дальність дії рознесеної двохпозиційної РМС $R_i(S,T)$ в залежності від площини об'єкту S та його температури T

Перша крива $R\left(10^2,T\right)$ на рис. 4 безперервна, відображає значення дальності дії РМС при зміні T (105-348 K), коли $S = \ = 10^2$ м^2. Так, наприклад $R\left(10^2,194\right) \approx \ \approx 5442$ м. При цьому під носієм на зображенні є N_τ різниць ходу через 0,5 ВКФ ($N_\tau \approx 6,3$) та відстань між різницями ходу $\Delta_\tau \approx 27,2$ м. Якщо $T \approx T_з$ то R_i прямує до нуля, так як відсутній радіояскравий контраст на поверхні зображення.

Смуга картографування $П_к$ визначаємо приблизно, при умові, що сканування антенною системою ведеться через напівширин її ДС $\Theta_{0,5}$, так:

$$П_к \approx \frac{2\left[R_i(S,T)\,\mathrm{tg}\left(\Theta_{0,5}/2\right)\right]^2}{V\,\tau_н}, \qquad (20)$$

де V – швидкість польоту носія (125 м/с); причому $\Theta_{0,5} = \sqrt{2}\,\lambda/L_i$.

Коли $R\left(10^2,194\right)$ отримали $П_к \approx 3020$ м.

При виявленні вологого ґрунту на фоні піску (гравію) величини $R(S,194)$ (четверта крива, точки тире на рис. 4) надає значення R_i, якщо перемінна S.

Доплерівська поправка частоти сигналу МО $F_д$ при двохпозиційній системі прийому та фіксованій висоти її прольоту дорівнює [2, 3, 10]:

$$F_д = \frac{2V}{\lambda}\sin\varepsilon\,\sin\left(\frac{\xi}{2}\right), \qquad (21)$$

де V – різниця швидкості між носієм (рис. 1) та МО на поверхні картографування; ε – кут між лінією МО – середина бази та вектором $\vec{V}$; ξ – кут, який створений першим пунктом прийому ПІ – МО – другим пунктом прийому ПІІ.

Якщо на кожному відведенні РМС (рис. 2) після квадратичних детекторів (квадраторів) встановлені, наприклад, 10 (N) фільтрів то $П_{вих}$ дорівнює 31 Гц. За рахунок недостатньої величини t (19) втрати в ν дорівнюють ~6,72 рази. Тобто у виразах (17), (18) нове значення ν, так $\nu = 5,64 \cdot 6,72 \approx 37,89$ рази.

Зміну величин ν у РМС, при звуженні $П_{вих}$, позначимо через B_i, яке знаходимо з виразу

$$B_i = \nu\left(П_{вих}\right)/\nu\left(П_{вих}/N\right), \qquad (22)$$

де N – кількість фільтрів Доплера на виході кожного з квадратичних детекторів (рис. 2).

Результати розрахунку за останнім виразом наведено на рис. 5. Нижня крива відображає зміну $B_i(t)$, коли $N=10$ та $\Pi_{\text{вих}}$ зменшується з 310 до 31 Гц, при цьому $t<3/\Pi_{\text{вих}}$ ($t<\tau_{\text{н}}$).

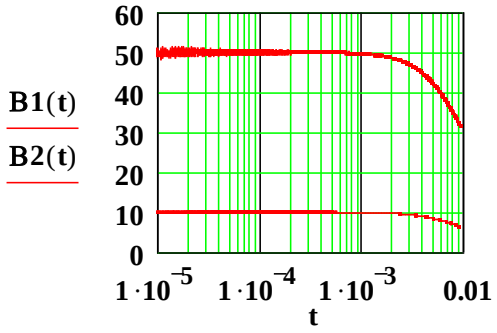


Рис. 5. Зміна співвідношення $B_i(t)$ за час інтегрування у радіометрі t, при звуженні смуги пропускання його вихідного фільтра $\Pi_{\text{вих}}$

Верхня крива на рис. 5 – $N=50$, $\Pi_{\text{вих}}$ зменшується з 310 до 6,2 Гц. Якщо $t<10^{-3}$ спостерігаємо на вказаних кривих власні шуми кореляційного радіометра.

Результати розрахунку $R_i(S,T)$ при вимірі $F_{\text{д}}$ надані другою кривою $R_1\left(10^2,T\right)$, яка позначена крапками на рис. 4. Дальність дії РМС зменшується ~1,57 рази відносно значення $R\left(10^2,194\right)$, так отримали $R_1\left(10^2,194\right)\approx 3464$ м. При цьому $\Pi_{\text{к}}\approx 1230$ м, $N_\tau\approx 6{,}3$ та $\Delta_r\approx 17{,}3$ м.

При встановленні 50 (N) фільтрів на виході кожного з квадратичних детекторів (рис. 2) отримуємо: $\Pi_{\text{вих}}=6{,}2$ Гц, $R_3\left(10^2,194\right)\approx 2320$ м, $N_\tau\approx 6{,}3$, $\Pi_{\text{к}}\approx 550$ м та $\Delta_r\approx 11{,}6$ м.

У РМС бажано мати прямокутний амплітудо-частотний спектр, тоді тіло невизначеності (ТН) на її виході $(\sin x/x)^2$ [8, 9]. Якщо значення $F_{\text{д}}$ у (21), наприклад, ~46 Гц, то рівень фону ТН, що заважає картографуванню, зменшується ~ -13 дБ. При збільшенні величини $F_{\text{д}}$ ~170 Гц, рівень фону ТН знижується до ~ -25 дБ. Вказане зменшення корельованого фону ТН, що заважає картографуванню, враховується множення (14) на $10^{-1{,}3}$ ($10^{-2{,}5}$) разів.

Третя крива $R_2\left(10^2,T\right)$ на рис. 4 позначена тире, відображає зміну значень відстані картографування, коли $F_{\text{д}}$ ~46 Гц. Відносно $R_1\left(10^2,T\right)$ дальність збільшується, так $R_2\left(10^2,194\right)\approx 4378$ м. П'ята крива $R_2(S,194)$ (○○○, рис. 4) також здобута якщо $F_{\text{д}}$ ~46 Гц. Відмічаємо, що крива $R(S,194)$ проходить вище $R_2(S,194)$. Втрати у дальності при виміру $F_{\text{д}}$ дорівнюють $R\left(10^2,T\right)\Big/R_2\left(10^2,T\right)\approx 1{,}24$ рази.

Картографування земної поверхні в ІЧ діапазоні довжин хвиль (3,3 – 4,2 мкм) при $\text{Б}=20$ м, R ~5,5 км надає $\Delta_r\approx 9\cdot 10^{-3}$ м.

Картографування космічних об'єктів. Якщо проводиться картографування космічних об'єктів з надземної орбіти, записи рівнянь $T_{\text{а}}$ (3) та $T_{\text{ф}}$(10) декілька змінюються:

$$T_{\text{а}}=(1-\beta_1)\eta\left(T_{\text{к}}+T\delta+\sum_{i=1}^{n}t_i\delta_i\right)+\beta_2\eta\left(T_{\text{атм}}+T_{\text{з}}+\sum_{j=1}^{k}t_j\delta_j\right)+(1-\eta)T_{\text{с}},$$
$$T_{\text{ф}}=(1-\beta_1)\eta\left(T_{\text{к}}+\sum_{i=1}^{n}t_i\delta_i\right)+\beta_2\eta\left(T_{\text{атм}}+T_{\text{з}}+\sum_{j=1}^{k}t_j\delta_j\right)+(1-\eta)T_{\text{с}}. \qquad (23)$$

де β_1, β_2 – відповідно частка ненаправленого випромінювання, які приймаються антеною радіометра у передній та задній напівсферах; $T_к, T_с$ – радіояскраві температури космосу та середи, що оточує антени відповідно.

Нове значення γ здобули перетворюючі вирази (11), (12) з врахуванням (2) – (7), так

$$\gamma = \frac{(1-\beta_1) S G T}{4\pi\alpha R^2 L\left[T_с (K_ш - \eta) + \mu (K_ш - 1) + A_1\right]}, \qquad (24)$$

де μ – різниця між значеннями T_0 та $T_с$;

$$A_1 = \eta\left[(1-\beta_1)\left(T_к + \sum_{i=1}^{n} t_i \delta_i\right) + \beta_2\left(T_{атм} + T_з + \sum_{j=1}^{k} t_j \delta_j\right)\right]$$

У підсумку отримуємо замість (18) варіант рівняння дальності спостереження за космічними об'єктами з надземної орбіти

$$R = \sqrt{\frac{T S G (1-\beta_1)}{4\pi\alpha\gamma L\left[T_с (K_ш - \eta) + \mu (K_ш - 1) + A_1\right]}}. \qquad (25)$$

Якщо є різниця між швидкостями надземного носія та космічного об'єкта картографування (21) величина A_1 в (25) зменшується відповідно $F_д$ та ТН фону, що корельовано.

Перспективним є побудова рознесених радіометричних систем при дослідженні космічних об'єктів в диапазонах від дециметрових до ІЧ довжин хвиль.

Висновки

Запропоновано підвищення чутливості та розрізнювальної здатності за різницею ходу за рахунок впровадження у кореляційний радіометр (рис. 2) відповідних модуляторів вхідних сигналів та квадратичних детекторів. Отримано рівняння дальності дії рознесеної двохпозиційної РМС з врахуванням радіояскравих температур атмосфери та поверхонь, що заважають. При типових технічних характеристиках РМС та виявленні вологого ґрунту з температурою T (~194K) площиною S (10^2) на однорідному фоні (~252K) отримали дальність дії R_i ~5,4 км. При цьому смуга картографування $П_к$ ~ 3 км, у кожному пікселі зображення різниць ходу N_τ ~6, а відстань між нами на поверхні Δ_r ~27 м. Вимірювання доплерівської поправки частоти $F_д$ при 10 вихідних фільтрах зменшує R_i до ~3,5 км і встановлює $П_к$ ~1,2 км, Δ_r ~17 м та N_τ ~6. Останні значення визначені за умови, що $F_д$ об'єкта співпадає з головною пелюсткою ТН фону, що корельовано. При зростанні $F_д$ у 1,5 рази рівень фону, що заважає, зменшується у ~ -13 дБ і R_i збільшується ~1,26 рази, так: R_i ~4,4 км, $П_к$ ~2 км, Δ_r ~22 м.

Запропоновано варіант визначення дальності дії рознесеної двохпозиційної РМС для картографування космічних об'єктів з надземної орбіти. Вказано на збільшення R_i при вимірі $F_д$, за рахунок зниження фону, що корельовано.

Список литературы : 1. *Теоретические* основы радиолокации / А.А. Коростелев, Н.Ф. Клюев, Ю.А. Мельник и др. ; под ред. В.Е. Дулевича. – 2-е изд. перераб. и доп. – М. : Сов. радио, 1978. – 608с. 2. *Алмазов В.Б.* Методы пассивной радиолокации. – Харьков : ВИРТА, 1974. – 86с. 3. *Караваев В.В., Сазонов В.В.* Статистическая теория пассивных радиолокационных систем. – М. : Радио и связь, 1987. – 240с. 4. *Биков В.Н.* Виявлення малорозмірних об'єктів радіометричною інформаційною системою мм діапазону з шумовою підсвіткою / Биков В.Н. // Радіоелектронні і комп'ютерні системи 2(10). –Харків : ХАІ. – 2005. – С. 5-11. 5. *Калинкин С.И., Кудряшов В.Е.,*

Хоменко Е.В. Выбор параметров многоканальной радиометрической системы обнаружения малоразмерных неоднородностей // Радиотехника. – 1992. – №10-11. – С. 3-7. 6. *Коломійцев О.В., Клеваний Ю.А., Мельников І.В.* Дальність радіотеплолокаційного спостереження двохпозиційною радіометричною системою повітряних цілей // Системи обробки інформації. – Харків : ХУПС, 2014. – Вип. 2(118). – С. 21 – 24. 7. *Lukin K.A., Kudriashov V.V., Vyplavin P.L., Palamarchuk V.P.* Coherent imaging in the range-azimuth plane using a bistatic radiometer based on antennas with beam synthesizing // IEEE Aerospace and Electronic Systems Magazine, 29, 7, pp. 16 – 22. 8. *Lukin K.A., Kudriashov V.V., Vyplavin P.L., Palamarchuk V.P., Lukin S.K.* Coherent radiometric imaging using antennas with beam synthesizing // International Journal of Microwave and Wireless Technologies, 7, Spec. Iss. 3-4, pp. 453 – 458. 9. *Kudryashov V.V., Lukin K.A, Palamarchuk V.P, Vyplavin P.L.* Coherent radiometric imaging with a Ka-band ground-based synthetic aperture noise radar // Telecommunications and Radio Engineering. – 2013. – Vol. 72, No. 8. – p. 699-710. 10. *Kudriashov V.V.* 'A Modified Maximum Likelihood Method for Estimation of Mutual Delay and Power of Noise Signals by Bistatic Radiometer '. Comptes Rendus – Academie Bulgarie des Sciences, 68, 5, pp. 631 – 640. 11. *Qingxia Li, Ke Chen, Wei Guo, Liang Lang, Fangmin He, Liangbing Chen*. An Aperture Synthesis Radiometer at Millimeter Wave Band // Microwave and Millimeter Wave Technology, 2008. ICMMT 2008. Vol. : 4, pp. 1699 – 1701. 12. *Ji Wu, Hao Liu, Shouzheng Ban, Xiaolong Dong, and Jingshan Jiang*. Research Activity on Synthetic Aperture Radiometry in CSSAR/CAS // Progress In Electromagnetics Research Symposium 2005. PIERS Vol. :1, No : 5, pp : 538-542. 13. *Дальність* радіотеплолокаційного спостереження кореляційним виявлячем сигналів малорозмірних об'єктів на поверхні землі / Коломійцев О.В., Кудряшов В.В. // V наук. конф. ХУПС ім. І.Кожедуба «Новітні технології – для захисту повітряного простору» : наук.-техн. конф., 28-29 бер. 2009 р. : тези доп. – Харків : ХУПС, 2009. – С. 217. 14. *Теоретические* основы радиолокации ; под ред. Я.Д. Ширмана. – М. : Сов. радио, 1970. – 560с. 15. *Институт* электроники и связи АН Украины, 2017. – Ел. Доступ http : //www.mitris.com/files/Osnovnye napravleniya razrabotok.pdf. 16. *Справочник* по радиолокации ; под ред. М. Сколника. Т. 4. Радиолокационные станции и системы ; под ред. М.М. Вейсбена. – М. : Сов. радио, 1978. – 376с. 17. С*правочник* по радиолокации ; под ред. М. Сколника. Т. 2. Радиолокационные антенные устройства ; под ред. П.И. Дудника. – М. : Сов. радио, 1977. – 408с. 18. Р*адиоприемные* устройства / Ю.Т. Давыдов, Ю.С. Даничь, и др. ; под ред. А.П. Жуковского. – М. : Высш. шк., 1989. – 388с. 19. *Регламент* радиосвязи. Статьи. – Женева : Швейцария, 2016. – 441 с. 20. *Шевченко А.Ф.* Результати порівняльного аналізу характеристик спрямованості кільцевих фазованих антенних решіток для завдань створення багатопозиційних активно-пасивних РЛС // Системи обробки інформації. – Харків : ХУПС. – 2014. – Вип. №9(125). – С. 65–72. 21. *Статистическая* радиотехника / Т.В. Горяинов, А.Г. Журавлев, В.И. Тихонов ; под ред. В.И. Тихонова. – М. : Сов. радио, 1980. – 544с. 22. *Алмазов В.Б., Манжос В.М., Камчатний Н.И.* Упрощенный алгоритм обнаружения шумового сигнала в двухпозиционной системе пассивной локации // Известия высших учебных заведений. Радиоэлектроника. – 1987. – Т. 30. № 11. – С.20–24. 23. *Леонов І.Л., Присяжний А.Е., Сидоренко Д.С.* Визначення робочих характеристик приймальних пристроїв шляхом моделювання на ПЄОМ // Системи обробки інформації. – Харків : ХУПС. – 2014. – Вип. №1(117). – С. 30–32.

Харківський національний університет
повітряних сил імені Івана Кожедуба

Надійшла до редколегії 15.10. 2017

УДК 621.391

В.М. БЕЗРУК, д-р техн. наук, С.А. ИВАНЕНКО

ИССЛЕДОВАНИЯ МЕТОДОВ ОБНАРУЖЕНИЯ НЕИЗВЕСТНЫХ СИГНАЛОВ

Введение

В настоящее время внедрение новых радиосистем ограничивается загруженностью частотных диапазонов и недостаточно эффективным использованием частотного ресурса [1, 2]. Одним из решений данной проблемы стало появление стандарта IEEE 802.22, который определяет работу радиосистем на основе применения технологий когнитивного радио (КР) [3]. При этом осуществляется поиск частотных каналов, временно не используемых первичными (лицензионными) пользователями, и предоставление их вторичным пользователям. Для этого необходимо следить за изменением сигнально-помеховой обстановки в частотных каналах путем проведения автоматизированного радиомониторинга. В анализируемых частотных каналах возможны следующие ситуации [2]:

1. На фоне помехи не наблюдаются сигналы, которые существовали в предыдущие циклы обзора, что может быть признаком снятия с эксплуатации систем, излучающих эти сигналы.

2. На фоне помехи появились новые, но ранее известные сигналы, что является признаком появления излучающей системы, которая работала в данном частотном канале в предыдущие циклы обзора.

3. На фоне помехи появились новые ранее неизвестные сигналы, что может служить признаком работы новых нелицензионных систем в данном частотном канале.

Таким образом, в результате анализа наблюдений в анализируемых частотных каналах должно приниматься решение о действии либо смеси сигнала с шумом, либо только шума, что фактически представляет собой задачу обнаружения сигналов на фоне шума. После обнаружения сигналов в частотном канале необходимо принять решение: действует либо неизвестный сигнал, либо ранее известный сигнал и какой именно. В общем случае задача анализа сигнально-помеховой ситуации в анализируемых частотных каналах представляет достаточно сложную задачу обнаружения и распознавания заданных сигналов при наличии неизвестных сигналов. Следует отметить, что при радиомониторинге сигналы в частотных каналах носят, как правило, случайный характер. Поэтому возникает необходимость решения задач обнаружения и распознавания случайных сигналов на фоне шума. При этом имеет место априорная неопределенность относительно вероятностных характеристик сигналов и шума.

В статье рассмотрены особенности решения только задачи обнаружения сигналов на фоне шума в условиях априорной неопределенности. Известны разные методы обнаружения сигналов при неполных сведениях о сигналах: в частности энергетический метод, метод согласованной фильтрации, метод циклостационарной функции [4]. Эти методы обнаружения основаны на использовании тех или иных сведений об обнаруживаемом сигнале. Существуют также методы обнаружения сигналов при априорной неопределенности, которые основаны на использовании обучающих выборок сигналов и шума [5]. Однако особенностью задач обнаружения сигналов при радиомониторинге является отсутствие возможности получения информации о виде сигнала или обучающих выборок сигналов в силу разнообразия видов и изменения характеристик сигналов в разных частотных каналах [2]. Это ограничивает возможности использования указанных методов обнаружения сигналов при проведении автоматизированного радиомониторинга.

В данной статье анализируются неклассические методы обнаружения случайных сигналов с неизвестными характеристиками, которые основаны только на знании вероятностных свойств шума в анализируемом частотном канале [6].

Решающие правила обнаружения неизвестных сигналов

При обработке наблюдений в анализируемом частотном канале выдвигаются две гипотезы: H^1 – действует сигнал на фоне шума; H^0 – действует только шум. Полагается, что шум описывается многомерной плотностью распределения $W(\mathbf{x}/\boldsymbol{\alpha}^0)$, представленной L-мерным вектором дискретных отсчетов наблюдений $\mathbf{x}$, $\boldsymbol{\alpha}^0$ – неизвестный векторный параметр плотности распределения. Задается обучающая выборка реализаций шума $\{\mathbf{x}_r^0, r=\overline{1,n_0}\}$, которая может быть использована для оценивания неизвестного векторного параметра $\boldsymbol{\alpha}^0$. Информация о вероятностных характеристиках сигнала отсутствует. Необходимо решить задачу обнаружения неизвестного сигнала на фоне шума, заданного своей обучающей выборкой.

Для решения сформулированной задачи обнаружения неизвестного сигнала может быть использовано следующее решающее правило [6]:

$$H^1: \ W(\mathbf{x}/\boldsymbol{\alpha}^0) > \lambda \ – \text{принимается гипотеза о наличии сигнала,} \quad (1а)$$

$$H^0: \ W(\mathbf{x}/\boldsymbol{\alpha}^0) \le \lambda \ – \text{отвергается гипотеза о наличии сигнала,} \quad (1б)$$

где λ – некоторое пороговое значение, выбираемое из условия обеспечения заданной вероятности ложной тревоги.

С учетом аналитического выражения для гауссового распределения вектора наблюдений $\mathbf{x}$ принятие решений с помощью решающего правила (1) сводится к сравнению с порогом малаханобисового расстояния вектора наблюдений $\mathbf{x}$ до эталона в сигнальном пространстве [6]:

$$H^1: (\mathbf{x}-\boldsymbol{\mu}^0)^{tr}(\mathbf{R}^0)^{-1}(\mathbf{x}-\boldsymbol{\mu}^0) > \Delta^0, \quad (2а)$$

$$H^0: (\mathbf{x}-\boldsymbol{\mu}^0)^{tr}(\mathbf{R}^0)^{-1}(\mathbf{x}-\boldsymbol{\mu}^0) \le \Delta^0, \quad (2б)$$

где $\boldsymbol{\mu}^0, \mathbf{R}^0$ – оценки среднего вектора и корреляционной матрицы, определяющие эталон, которые могут быть получены по обучающей выборке шума; Δ^0 – некоторое пороговое значение.

В частности, решающее правило типа (2) может быть получено также и в спектральной области, когда наблюдения $\mathbf{x}$ представляется вектором коэффициентов разложений $\mathbf{b}$ в некотором ортонормированном базисе:

$$H^1: (\mathbf{b}-\boldsymbol{\mu}^0_{\mathbf{b}})^{tr}(\mathbf{R}^0_{\mathbf{b}})^{-1}(\mathbf{b}-\boldsymbol{\mu}^0_{\mathbf{b}}) > \Delta^0_{\mathbf{b}}, \quad (3а)$$

$$H^0: (\mathbf{b}-\boldsymbol{\mu}^0_{\mathbf{b}})^{tr}(\mathbf{R}^0_{\mathbf{b}})^{-1}(\mathbf{b}-\boldsymbol{\mu}^0_{\mathbf{b}}) \le \Delta^0_{\mathbf{b}}, \quad (3б)$$

где $\mathbf{b}$, $\boldsymbol{\mu}^0_{\mathbf{b}}$, $\mathbf{R}^0_{\mathbf{b}}$ – отображение параметров соответственно $\mathbf{x}$, $\boldsymbol{\mu}^0$, $\mathbf{R}^0$ в спектральную область, определяемую выбранным ортонормированным базисом.

Для случая гауссового распределения и некоррелированности координат векторов наблюдений во временной либо спектральной области решающее правило обнаружения неизвестных сигналов представляется в виде соотношений [6]:

$$\sum_{j=1}^{N}\frac{(c_j-\mu^0_{jc})^2}{(\sigma^0_{jc})^2} > \Delta^0_c; \quad H^0: \sum_{j=1}^{N}\frac{(c_j-\mu^0_{jc})^2}{(\sigma^0_{jc})^2} \le \Delta^0_c, \quad (4)$$

где c_j – координаты векторов наблюдений, μ^0_{jc} – оценки математических ожиданий и дисперсий координат c_j, Δ^0_c – некоторые пороговые значения, выбираемые из условия обеспечения заданной вероятности ложной тревоги.

Если решение принимается по выборке наблюдений объемом ν реализаций, решающее правило (4) принимает вид:

$$H^1: \sum_{r=1}^{\nu}\sum_{j=1}^{N}\frac{(c_j-\mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} > \Delta_{c\nu}^0; \qquad H^0: \sum_{r=1}^{\nu}\sum_{j=1}^{N}\frac{(c_j-\mu_{jc}^0)^2}{(\sigma_{jc}^0)^2} \le \Delta_{c\nu}^0, \tag{5}$$

Возможны и другие варианты решающих правил обнаружения неизвестных сигналов, в частности по оценкам энергетических спектров наблюдений в некотором ортонормированном базисе.

Результаты исследований решающих правил обнаружения сигналов

Для исследования рассмотренных решающих правил была использована установка, которая включала SDR приемник, состыкованный с компьютером, и соответствующее программное обеспечение [7]. С помощью данной установки осуществлялось сканирование заданного диапазона частот и проводилась запись в оцифрованном виде выборок реализаций сигналов и шума, действующих в выбранных частотных каналах.

Получены обучающие и контрольные выборки реализаций сигналов и шума, наблюдаемых в частотных каналах с полосой 125 кГц в диапазоне частот стандарта IEEE 802.22. Была выбрана частота дискретизации наблюдений, равная 250 кГц. Накоплены обучающих и контрольных выборок сигналов и шума объем по 1000 реализаций, каждая из которых включала 256 дискретных отсчетов, взятых с частотой 250 кГц.

Полученные выборки наблюдений использованы для проведения исследований рассмотренных решающих правил обнаружения неизвестных сигналов. Исследования проводились методом статистических испытаний. При этом решающие правила были программно реализованы в среде MATLAB. Обучающие выборки реализаций шума использовались для оценивания неизвестных параметров исследуемых решающих правил. Контрольные выборки реализаций сигналов и шума использовались для получения оценок вероятностей правильного обнаружения сигналов на фоне шума в выбранном частотном канале.

Поскольку решающие правила обнаружения неизвестных сигналов основаны на использовании вероятностных свойств шума, вначале проведены исследования статистических характеристик шума в выбранном частотном канале. По обучающим выборкам шума построена гистограмма распределений его выборочных значений (рис. 1), а также найдены оценки корреляционной функции шума (рис. 2). Из анализа полученных результатов можно сделать предположение о гауссовом распределении выборочных значений шума, а также об их некоррелированности. Близкие результаты были получены по выборкам реализаций шума, действующего в других частотных каналах.

Полученные результаты исследований статистических характеристик шума дают основание использовать решающие правила обнаружения неизвестных сигналов (4), (5), которые основаны на предположениях о гауссовом распределении и некоррелированности выборочных значений шума.

Также были проведены исследования статистических характеристик шума в случае представления наблюдений $\mathbf{x}$ в ортонормированном базисе дискретных экспоненциальных функций (ДЭФ). При этом рассматривалось спектральное представление наблюдений шума в виде отсчетов амплитудного спектра в базисе ДЭФ. В результате анализа получено, что такое спектральное представление наблюдений шума подчиняется распределению Райса, которое при определенных условиях переходит в гауссово распределение. Вычислена также оценка корреляционной функции отсчетов амплитудного спектра шума, которая имеет вид близкий к рис. 2. Это дает основание использовать решающие правила обнаружения неизвестных сигналов (4), (5), основанные на гауссовом распределении и некоррелированности спектральных отсчетов шума.

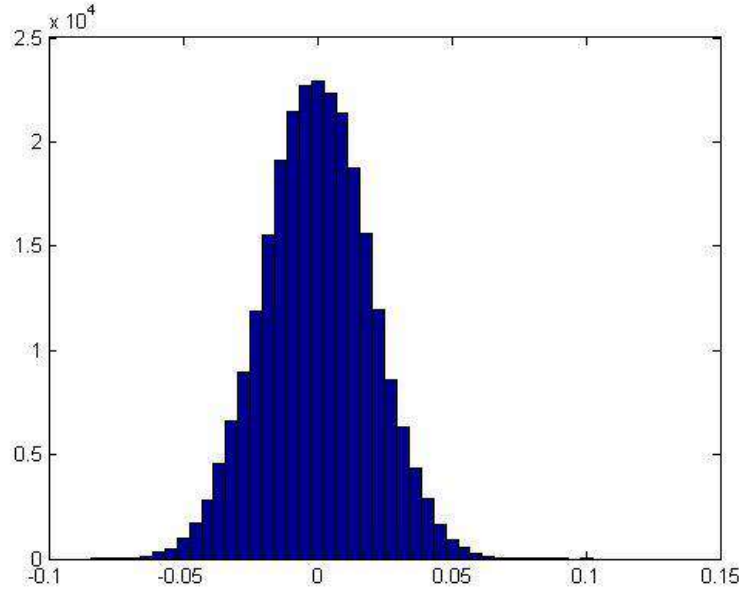


Рис. 1. Гистограмма распределений выборочных значений шума

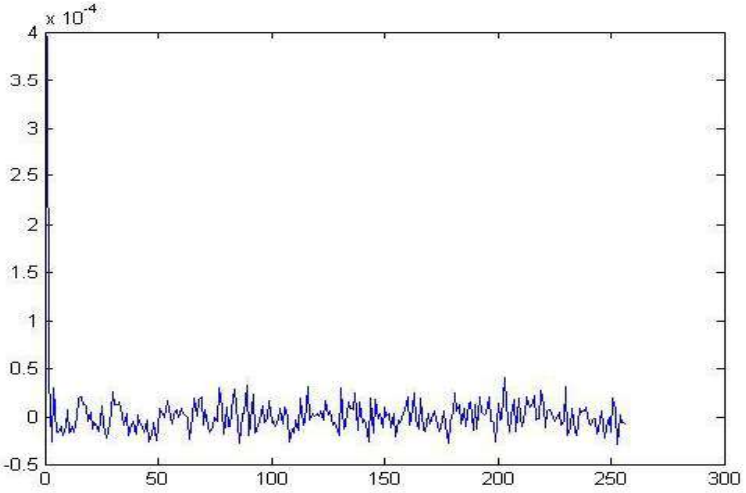
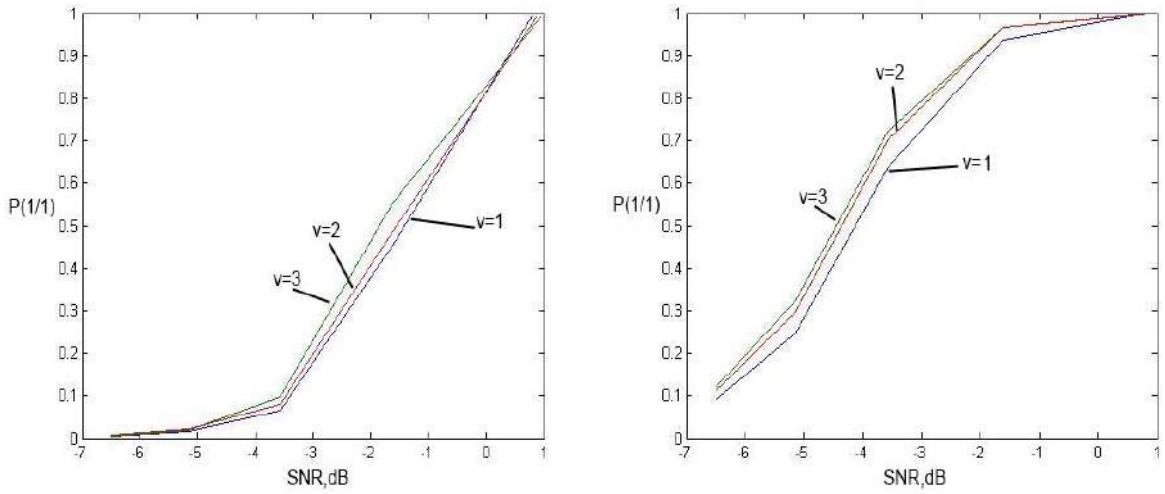


Рис. 2. Оценка корреляционной функции шума

С использованием накопленных выборок реальных сигналов, действующих в анализируемых частотных каналах, проведены сравнительные исследования рабочих характеристик обнаружения неизвестных сигналов на фоне шума для решающих правил обнаружения, реализованных во временной и спектральной области. На этапе обучения по накопленным выборкам шума находились параметры решающих правил. Пороговое значение Δ_c^0 выбиралось из условия обеспечения заданной вероятности ложной тревоги. В рабочем режиме подавались реализации наблюдений в виде аддитивной смеси сигнала и шума, действующих в выбранном частотном канале. Путем статистических испытаний с использований контрольных выборок реализаций сигналов были получены оценки вероятности правильного обнаружения неизвестных сигналов. Исследования проведены для разных типов сигналов, действующих в частотных каналах.

Для примера на рис.1 приведен амплитудный спектр одного из сигналов, который рассматривался как неизвестный сигнал, действующий на фоне шума в анализируемом частотном канале. Для этого случая проведены исследования рабочих характеристик обнаружения в виде зависимости оценок вероятности правильного обнаружения $P(1/1)$ от соотношения сигнал-шум (ОСШ) SNR. Оценки $P(1/1)$ были получены как отношение числа опытов n, в

которых приняты правильные решения, к общему числу опытов N, равному объему контрольной выборки из 1000 реализаций. На рис. 3 приведены полученные зависимости для решающего правила (5), реализованного соответственно во временной и спектральной области при фиксированной вероятности ложной тревоги $P(1/0) = 0,04$. Оценки $P(1/1)$ были получены при разных значениях $\nu = 1,2,3$.



а *б*

Рис. 3. Зависимости оценок вероятности правильного обнаружения неизвестны сигналов от ОСШ во временной области (*а*) и спектральной области (*б*) при вероятности ложной тревоги $P(1/0) = 0,04$

Из анализа результатов исследований следует, что рассмотренные решающие правила могут быть использованы для решения задачи обнаружения неизвестных сигналов на фоне шума в анализируемых частотных каналах. При этом могут быть достигнуты приемлемые значения вероятности правильного обнаружения неизвестных сигналов путем выбора необходимого ОСШ. Также видно, что переход к представлению наблюдений в спектральной области в виде отсчетов амплитудного спектра в базисе ДЭФ обеспечивает существенно большие значения вероятности правильного обнаружения неизвестных сигналов при прочих равных условиях по сравнению с временным представлением наблюдений.

Выводы

1. Рассмотрены нетрадиционные методы обнаружения неизвестных сигналов, действующих на фоне шума в анализируемом частотном канале. Методы обнаружения базируются на решающих правилах, в которых используется информация только о статистических характеристиках шума. Неизвестные статистические характеристики шума могут быть оценены по соответствующей обучающей выборке помехи.

2. Исследования решающих правил обнаружения неизвестных сигналов проведены методом статистических испытаний на выборках реальных сигналов и шума, полученных с использованием установки, которая включала сканирующий приемник и специальное программное обеспечение.

3. Исследованы статистические характеристики шума, действующие в частотных каналах. В частности, построены гистограммы распределений и получены оценки корреляционных функций выборочных значений шума. Их анализ показывает, что можно предполагать гауссово распределение и некоррелированность отсчетов шума. Это дает основание использовать соответствующие решающие правила обнаружения неизвестных сигналов.

4. Проведены сравнительные исследования решающих правил обнаружения неизвестных сигналов на фоне шума, представленных как во временной области, так и в спектральной области в виде амплитудного спектра в базисе ДЭФ. С использованием выборок реальных сигналов и шума методом статистических испытаний получены характеристики обна-

ружения неизвестных сигналов в виде зависимостей оценок вероятности правильного обнаружения от соотношения сигнал-шум при фиксированной вероятности ложной тревоги.

5. Полученные результаты исследований характеристик обнаружения свидетельствуют о возможности применения предложенных решающих правил для обнаружения неизвестных сигналов в частотных каналах при автоматизированном радиомониторинге. Это позволит решать задачи анализа сигнально-помеховых ситуаций с целью выявления незанятых частотных каналов в рамках технологии когнитивных радиосетей.

Список литературы: 1. *Реєстр* присвоєнь радіочастот (централізовані присвоєння) [Электронный ресурс] // УДЦР. – Режим доступа: http://www.ucrf.gov.ua/ 2. *Коханович, Г. Ф., Бабак, В.П., Фисенко, В.М.* Специальный радиомониторинг. – Киев : МК-Прес, 2007. – 384 с. 3. *Haykin S.* Cognitive Radio: Brain-empowered Wireless Communications // IEEE Journal on Selected Areas in Commun. – 2005. – Vol. 23, No. 2. – pp. 201-220. 4. Mata-*Moya D. de la, Jarabo-Amores M. P., Rosa-Zurera M., Nieto Borge J. C. and Lopez-Ferreras F.* Combining MLPs and RBFNNs to Detect Signals With Unknown Parameters // IEEE Transactions on Instrumentation and Measurement. – 2009. – Vol. 58, No. 9. – pp. 2989-2995. 5. *Теория* обнаружения сигналов / П.С. Акимов, П.А. Бакут, В.А. Богданович и др. – М. : Радио и связь, 1984. – 440 с. 6. *Безрук В.М., Певцов Г.В.* Теоретические основы проектирования систем распознавания сигналов для автоматизированного радиоконтроля. – Харьков : Коллегиум, 2007. – 430 с. 7. *SDR* and CR Boost Wireless Communications [Электронный ресурс] // Режим доступа: http://www.electronicdesign.com

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 07.10.2017

УДК 621.396.96:504.064.3

Б.В. ПЕРЕЛЫГИН, канд. техн. наук, А.М. ЛУЖБИН, канд. геогр. наук

ПОСТРОЕНИЕ СПЛОШНОГО РАДИОЛОКАЦИОННОГО ПОЛЯ СИСТЕМЫ ГИДРОМЕТЕОРОЛОГИЧЕСКОГО МОНИТОРИНГА НА ОСНОВЕ ГЕОМЕТРИЧЕСКОГО ПОДХОДА

Введение

Вопросам создания метеорологических радиолокационных сетей в литературе уделяется достаточное внимание [1 – 6]. Но анализ источников показывает, что при их создании не рассматриваются вопросы построения радиолокационного поля. Созданию единого радиолокационного поля уделяется внимание при проведении военной деятельности [7]. Но единство поля в этом случае понимается как интеграция радиолокационных ресурсов разных ведомств, их совместное использование с целью уменьшения необходимого для создания радиолокационного поля количества радиолокационных станций, т.е. с целью экономии. Создание системы гидрометеорологического мониторинга как большой системы подразумевает построение потребного радиолокационного поля [8]. Под этим нужно понимать следующее: во-первых, сформированное радиолокационное поле должно быть сплошным или беспровальным, т.е. полностью и без провалов покрывать пространство наблюдений; во-вторых, сформированное радиолокационное поле должно быть устойчивым, т.е. при выходе из строя или подавлении помехами некоторой части радиолокаторов целостность поля не должна нарушаться или может уменьшиться на некоторую допустимую величину; в-третьих, сформированное радиолокационное поле должно быть многочастотным для обеспечения возможности реализации двухчастотного метода индикации града [9].

Статья посвящена созданию сплошного (беспровального) радиолокационного поля системы гидрометеорологического мониторинга, что, в случае реализации, позволит получить всю возможную радиолокационную информацию из пространства наблюдений. Объектом исследования является процесс радиолокационного гидрометеорологического мониторинга, а предметом исследования – радиолокационное поле, образуемое системой радиолокационного гидрометеорологического мониторинга.

Актуальность решения этой задачи сомнений не вызывает, поскольку наличие правильно построенной радиолокационной системы гидрометеорологического мониторинга и правильное использование полученной с ее помощью информации значительно повышает качество прогнозирования состояния атмосферы оперативными подразделениями службы погоды [10].

Цель и метод исследования

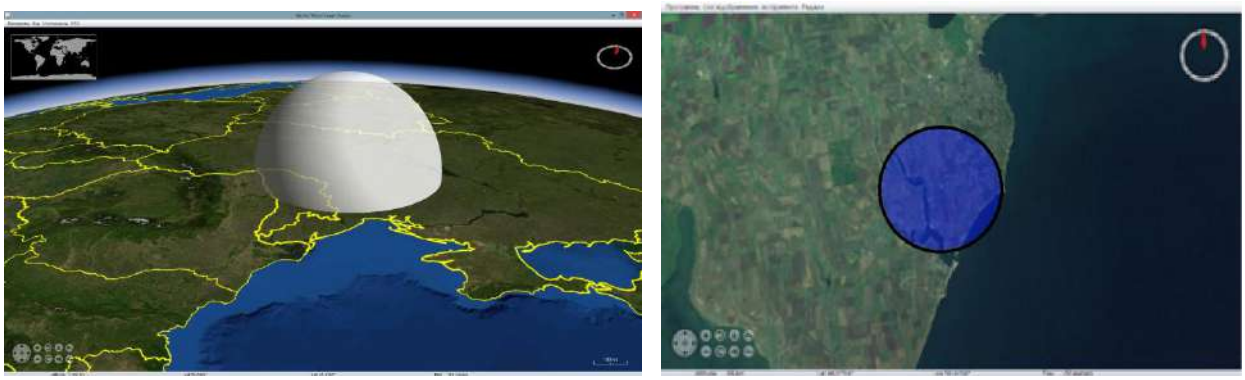
Цель исследования – обоснование необходимости применения геометрического подхода к построению радиолокационного поля системы гидрометеорологического мониторинга – достигается на основе применения метода сравнительного анализа и количественной оценки параметров моделей различных вариантов построения радиолокационного поля.

Описание исследования и анализ его результатов

Пространство наблюдений является той частью воздушного пространства, в которой существуют атмосферные объекты, явления и процессы, подлежащие радиолокационному мониторингу. Геометрически пространство наблюдений можно представить в виде цилиндрического объема, образующая которого проходит по границам исследуемой территории, а сверху и снизу этот объем ограничен плоскими основаниями, построенными на минимальной и максимальной потребной высоте (рис. 1). Минимальная потребная высота для радиолокационного поля системы гидрометеорологического мониторинга должна составлять около 0,5 км, а максимальная – до 20-25 километров [11].

Рис. 1

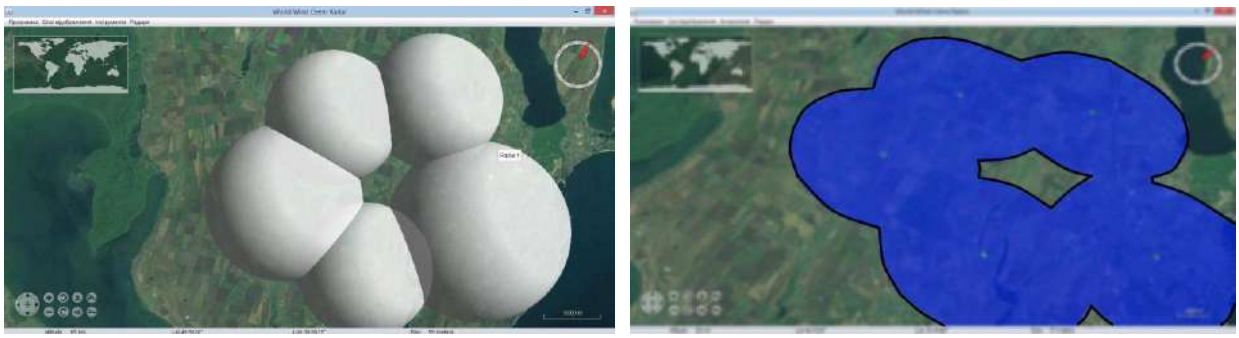
Построение сплошного радиолокационного поля предусматривает полное и наиболее точное покрытие им пространства наблюдений. Осуществляется это покрытие при помощи распределения зондирующего излучения в пространстве наблюдений и приеме из него сигналов, отраженных от метеорологических объектов и явлений. Зондирующее излучение в пространстве распределяется с помощью антенных систем. Понятно, что при большом пространстве наблюдений распределить в нем зондирующее излучение одной антенной не удастся. Нужна система антенн, т.е. множество радиолокационных станций, которые будут осуществлять обзор при помощи антенн. В этом случае одна радиолокационная станция образует зону обзора или зону наблюдения (на рис. 2, *а* – трехмерное изображение зоны обзора, на рис. 2, *б* – вертикальная проекция горизонтального сечения зоны обзора на определенной высоте). А множество радиолокационных станций образуют радиолокационное поле (рис. 3, *а* – трехмерное изображение радиолокационного поля, рис. 3, *б* – вертикальная проекция горизонтального сечения радиолокационного поля на определенной высоте). Возникает вопрос: каким образом расположить метеорологические радиолокационные станции для создания радиолокационного поля?



а *б*

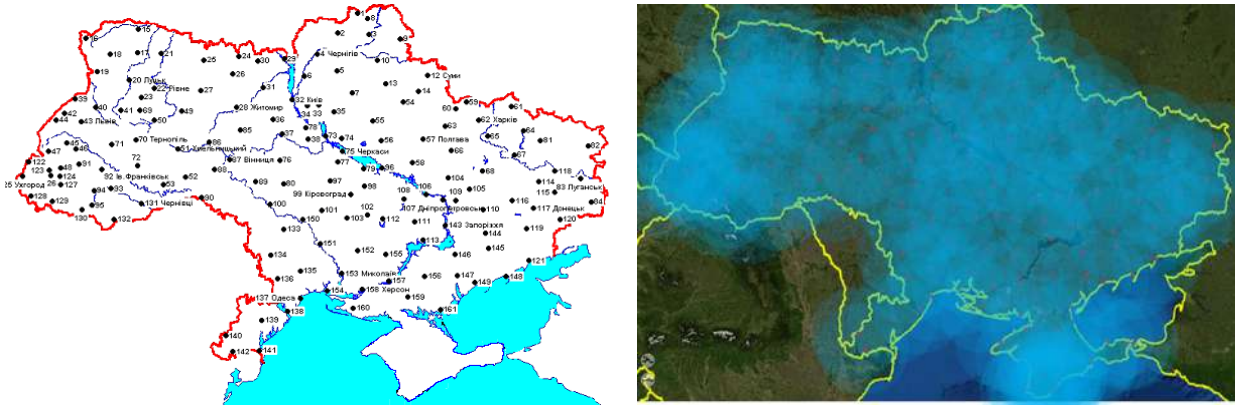
Рис. 2

Моделирование показывает, что желание оснастить радиолокатором каждую гидрометеорологическую станцию (рис. 4, *а*) приведет к получению ничем не оправданной сложности и энергетической избыточности системы мониторинга. Система будет иметь очень неравномерное распределение зондирующего излучения, а при сборе и отождествлении радиолокационной информации возникнут существенные трудности. Это хорошо иллюстрирует рис. 4, *б*. Зоны наблюдения многократно перекрываются, очень неравномерное распределение энергии в пространстве, что и будет вызвать упомянутые избыточность и сложность обработки информации.



а *б*

Рис. 3



а *б*

Рис. 4

Приведенный вариант построения радиолокационного поля можно выполнить с прореживанием радиолокаторов, но моделирование показывает, что недостатки от этого не исчезнут. При значительном прореживании и при сохранении позиций радиолокаторов привязанными к существующей сети гидрометеорологических станций увеличится минимальная высота радиолокационного поля. И избежать этого недостатка в существующей системе построения радиолокационной сети не удастся.

Предлагается применить для построения радиолокационного поля системы гидрометеорологического мониторинга геометрический подход. Он заключается в том, что радиолокаторы предполагается размесить в вершинах связанных простейших геометрических фигур – треугольников, квадратов, пятиугольников, шестиугольников и т.д. (рис. 5). Из геометрии известно, что сеть из пятиугольников и семиугольников нельзя без искажений выложить на плоскости [12]. Поэтому эти варианты размещения радиолокаторов рассматривать не будем, но в оценке параметров радиолокационного поля используем.

Реализация геометрического подхода при моделировании приводит к следующим результатам. Расположение радиолокаторов в вершинах треугольников обеспечивает полное перекрытие пространства наблюдений в горизонтальной плоскости и, при некотором сближении радиолокаторов, в вертикальной плоскости (рис. 6). При этом отсутствует существенная избыточность (сегменты более темного тона) по перекрытию в горизонтальной плоскости, свойственная предыдущему описанному случаю, но энергетическая избыточность в вертикальной плоскости будет существенной, и тем существенней, чем больше будет дальность действия радиолокатора, поскольку потребная высота верхней границы радиолокационного поля составляет всего 20-25 км.

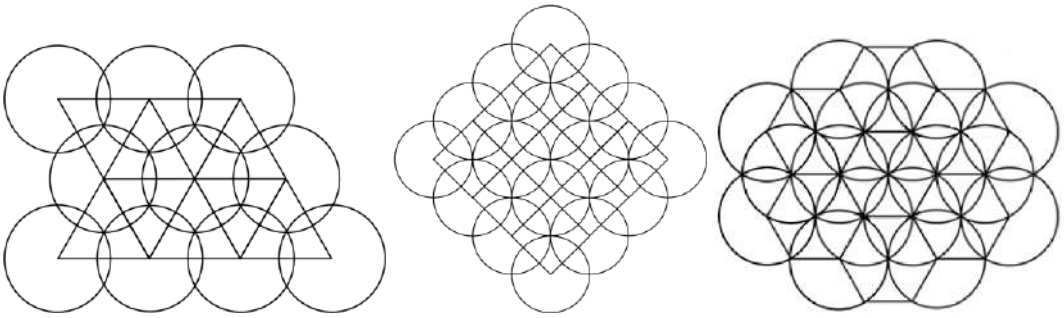


Рис. 5

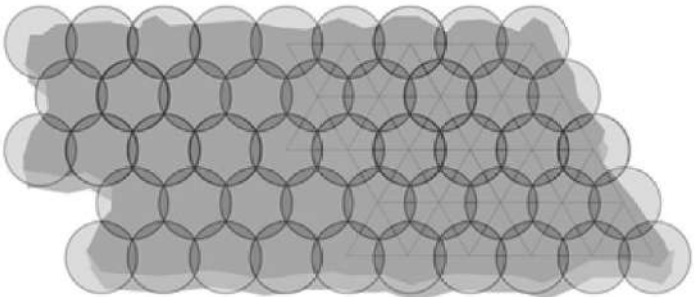


Рис. 6

Расположение радиолокаторов в вершинах квадратов также обеспечивает полное перекрытие пространства наблюдений в горизонтальной плоскости и, при некотором сближении радиолокаторов, в вертикальной плоскости (рис. 7). Однако при таком расположении видно явно большее перекрытие зон обзора радиолокаторов по сравнению с расположением в вершинах треугольников (более темные сегменты), что ухудшает энергетическую экономичность этого варианта построения радиолокационного поля.

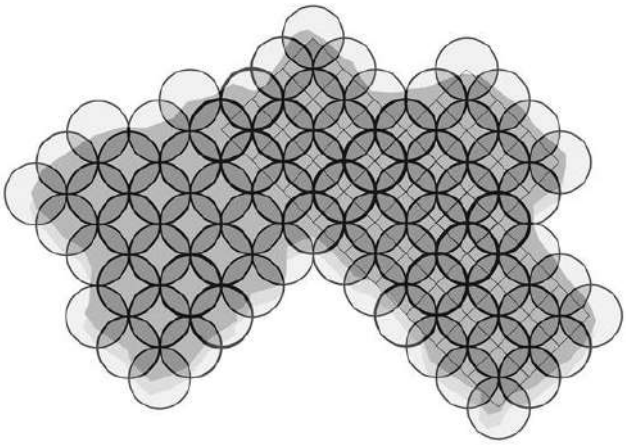


Рис. 7

Расположение радиолокаторов в вершинах шестиугольников также обеспечивает полное перекрытие пространства наблюдений в горизонтальной плоскости и, при некотором сближении радиолокаторов, в вертикальной плоскости (рис. 8). Но при подобном расположении явно видно еще большее, в середине практически полное, перекрытие зон обзора радиолокаторов по сравнению с предыдущими случаями (область серого тона), что еще больше ухудшает энергетическую экономичность этого варианта построения радиолокационного поля.

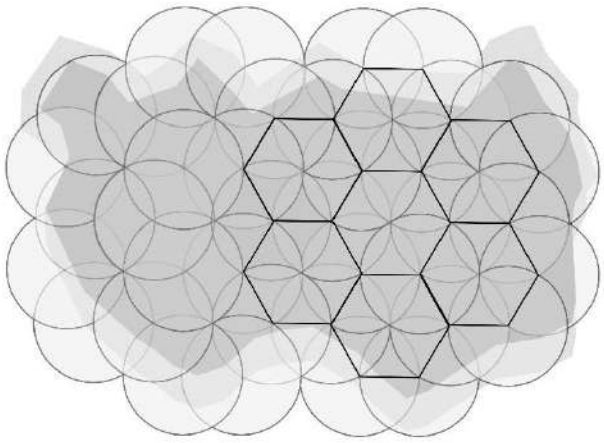


Рис. 8

При построении радиолокационного поля должна быть обеспечена его беспровальность начиная с минимальной требуемой высоты (0,5 км) до максимальной (20–25 км). Это достигается уменьшением сторон многоугольника до тех пор, пока в центре фигуры не произойдет касание зон обзора радиолокаторов, находящихся в вершинах многоугольника, как это видно на предыдущих рисунках. Тогда при дальности действия радиолокатора R сторона равностороннего треугольника должна быть равна 2Rcos30° или 1,732 R. Для других многоугольников данные приведены в табл. 1.

Таблица 1

Дальность действия радиолокатора	Расстояние между радиолокаторами (D=2RcosX°) для формирования беспровального радиолокационного поля при расположении радиолокаторов в вершинах						
	на концах отрезка прямой линии	равностороннего треугольника	квадрата	правильного пятиугольника	правильного шестиугольника	правильного семиугольника	правильного восьмиугольника
	X°=0°	X°=30°	X°=45°	X°=54°	X°=60°	X°=64,3°	X°=67,5°
R	D=2·R	D=1,732·R	D=1,414·R	D=1,176·R	D=1·R	D=0,87·R	D=0,76·R

В результате анализа полученных данных можно прийти к выводу о том, что для построения радиолокационного поля нецелесообразно выбирать многоугольник с числом вершин (порядок многоугольника) больше шести, поскольку, в противном случае, начинают взаимно накладываться зоны обзора не только смежных радиолокаторов, но и далеко отстоящих друг от друга. А это – явная энергетическая избыточность и усложнение обработки из-за необходимости отождествления данных. Таким образом, при построении радиолокационного поля целесообразными остаются три варианта размещения радиолокаторов: в вершинах треугольников, квадратов и шестиугольников; пятиугольники отпадают по указанной ранее причине.

Для построения радиолокационного поля по приведенным выше вариантам качественной оценки недостаточно, нужна количественная оценка качества поля. Поэтому для количественной оценки энергетических характеристик поля представляет интерес выяснение коэффициента перекрытия радиолокационного поля и его энергетической экономичности в зависимости от варианта размещения радиолокаторов. Коэффициентом перекрытия $К_п$ вполне логично назвать отношение суммарного объема зон наблюдения, обслуживаемого более чем одной радиолокационной станцией, к общему объему зон наблюдения, т.е.

$$К_п = \frac{\sum_1^n V_{совм}}{\sum_1^n V_{ЗН}}, \quad (1)$$

где $V_{совм}$ – объем области пространства, обслуживаемого двумя соседними радиолокаторами; $V_{ЗН}$ – объем зоны наблюдения одного радиолокатора, n – порядок многоугольника.

При такой трактовке при полном совмещении позиций радиолокаторов $К_п$=1, а если зоны наблюдения не пересекаются, то $К_п$=0, что является вполне естественным.

Проверка практического применения этого коэффициента выявила ненужную сложность его расчета. Гораздо удобнее проводить расчеты, если использовать показатель перекрытия вертикальных проекций горизонтальных сечений зон наблюдения радиолокаторов на минимальной беспровальной высоте. В этом случае в (1) объемы заменяются на соответствующие площади вертикальных проекций этих объемов на горизонтальную плоскость, но смысл понятия перекрытия от этого не изменяется. Логично назвать такой показатель коэффициентом перекрытия в горизонтальной плоскости $К_{пг}$, т.е.

$$К_{пг} = \frac{\sum_1^n S_{совм}}{\sum_1^n S_{ЗН}}, \quad (2)$$

где $S_{совм}$ – площадь проекции области пространства, обслуживаемого двумя соседними радиолокаторами, $S_{ЗН}$ – площадь проекции зоны наблюдения одного радиолокатора, n – порядок многоугольника.

Для расчета $К_{пг}$ были применены известные из геометрии формулы для расчета площади круга $S_{кр}=\pi R^2$ и площади сегмента $S_{сегм} = \frac{R^2}{2}\left(\pi\frac{\alpha^\circ}{180^\circ} - \sin\alpha^\circ\right)$ [12]. Здесь R – дальность действия радиолокатора, α – центральный угол, который опирается на сегмент, образующийся при пересечении двух зон обзора радиолокаторов. Расчеты для α дали результаты, представленные в табл. 2.

Таблица 2

Расположение радиолокаторов в вершинах			
равностороннего треугольника	квадрата	правильного пятиугольника	правильного шестиугольника
α = 60°	α = 90°	α = 108°	α = 120°

Дальнейшие расчеты позволили графически представить зависимость $К_{пг}$ от порядка многоугольника (рис. 9).

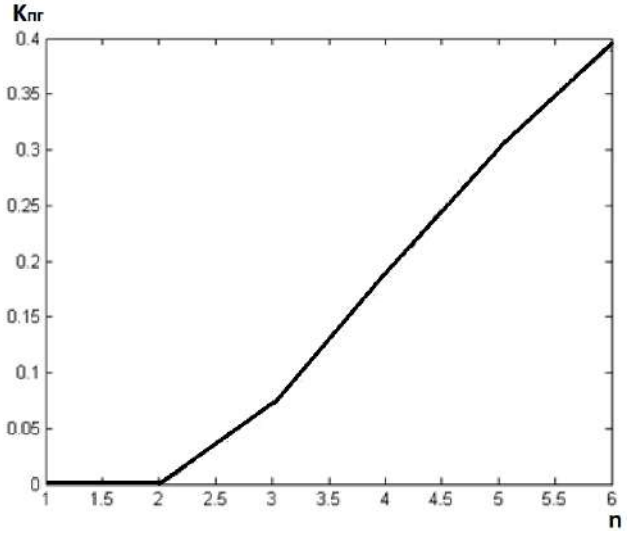


Рис. 9

Ход коэффициента перекрытия отражает то, что увеличение порядка многоугольника, в вершинах которых устанавливаются радиолокаторы, ведет к увеличению доли радиолокационного поля, обслуживаемой двумя, а то и тремя радиолокаторами, тем самым увеличивая непроизводительные затраты зондирующего излучения. Это обязательно надо учитывать при построении радиолокационного поля.

Как было отмечено выше, представляет интерес выяснение вопроса экономности распределения энергии зондирующего излучения внутри радиолокационного поля при взаимном наложении зон наблюдения радиолокаторов. Можно степень экономности характеризовать коэффициентом экономности $К_э$. Этот коэффициент должен быть равен единице при отсутствии взаимного наложения зон наблюдения и нулю при полном наложении. Поскольку экономность связана с взаимным перекрытием зон наблюдения, то решением является введение коэффициента $К_э=1–К_{пг}$. Ход этого коэффициента в зависимости от порядка многоугольника приведен на рис. 10.

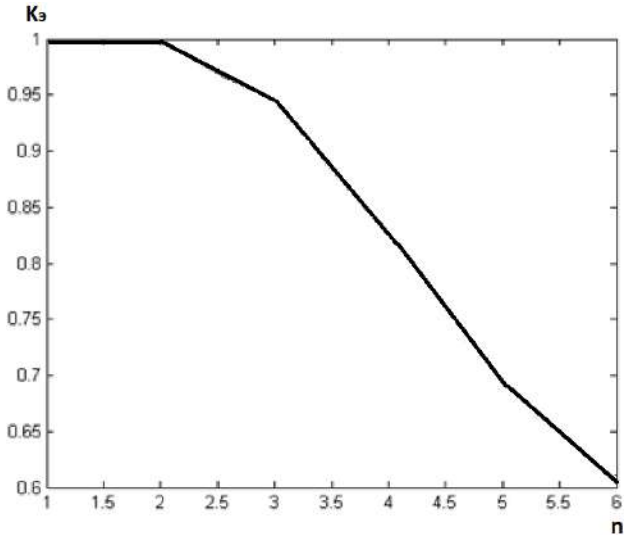


Рис. 10

Анализ графика на рис. 10 показывает, что отдельно стоящие радиолокаторы будут использовать энергию зондирующего излучения в наибольшей степени экономно (без учета вертикального распределения энергии). А при расположении их в вершинах шестиугольников только 60 % радиолокационного поля будет обслуживаться экономно, в остальной его части объекты, явления и процессы будут наблюдаться двумя радиолокаторами и более.

Выводы

Исследование показало, что применение геометрического подхода к построению радиолокационного поля метеорологической радиолокационной системы мониторинга позволяет достаточно просто получить результат. Наиболее рациональным является размещение радиолокаторов в вершинах треугольников, квадратов и шестиугольников. Выбор варианта размещения позволит удовлетворить различные требования к метеорологической радиолокационной системе мониторинга: от наиболее экономного варианта расходования энергии зондирующего излучения до наиболее устойчивого варианта построения системы.

Список литературы: 1. *European* Commission, EUR 18567, „COST 75 – Advanced weather radar systems – International seminar", ed. C.G. Collier, Luxemburg, Office for official publications of the European Communities. – 1999. – 858 p. 2. *Технический* проект „Общесистемные решения по сбору, анализу, контролю и предоставлению радиолокационной информации от ДМРЛ-С". – Режим доступа: http://www.aviamettelecom.ru/TP-DMRL-2014.pdf. – Дата доступа: 15.09.2016. – Технический проект. 3. *Golden J.H.* The prospects and promise of

NEXRAD: 1990's and beyond / J.H. Golden // COST 73. – 1989. – P. 17–36. 4. *Принципы* построения автоматизированных систем метеорологического обеспечения авиации ; под ред. Г.Г. Щукина. – Л. : Гидрометеоиздат, 1991. – 373 с. 5. *Метеорологические* автоматизированные радиолокационные сети ; под ред. Г.Б. Брылева. – С.-Пб. : Гидрометеоиздат, 2002. – 330 с. 6. *Радиолокационные* метеорологические наблюдения. В 2-х т. Т.2 ; под ред. А.С. Солонина. – С.-Пб. : Наука, 2010. – 518 с. 7. *Петрушенко, М.М., Карлов, В.Д.* Створення єдиного поля радіолокаційного контролю повітряного простору держави // Наука і техніка Повітряних Сил Збройних Сил України. – 2010. – № 1 (3). – С. 111–116. 8. *Perelygin, B.V.* Reasonable deployment of radar field for environmental monitoring system // Telecommunications and radio engineering. – 2016. – Vol. 75. № 9. – P. 823–833. Doi: 10.1615/TelecomRadEng.v75.i9.70. 9. *Абшаев, М.Т., Бурцев, И.И., Ваксенбург. С.И., Шевела. Г.Ф.* Руководство по применению радиолокаторов МРЛ-4, МРЛ-5 и МРЛ-6 в системе градозащиты. – Л. : Гидрометеоиздат, 1980. – 231 с. 10. *Грачова, Н.І., Кузнєцова, В.В., Романенко, Л.Н., Самаріна, Л.П.* Дослідження радіолокаційних характеристик небезпечних явищ погоди на території України // Наукові праці УкрНДГМІ. – 2015. – Вип. 267. – С. 38–45. 11. *Перелыгин, Б.В., Боровская. Г.А., Лужбин. А.М.* Анализ требований потребителей к характеристикам информации, получаемой от метеорологической радиолокационной системы мониторинга // Радиотехника. – 2016. № 187. – С. 58–65. 12. *Корн, Г., Корн, Т.* Справочник по математике для научных работников и инженеров. – М. : Наука, 1984. – 832 с.

Одесский государственный
экологический университет

Поступила в редколлегию 11.11.20117

УДК 629.7.022

В.М. КАРТАШОВ, д-р техн. наук, В.Н. ОЛЕЙНИКОВ, канд. техн. наук,
С.А. ШЕЙКО, канд. техн. наук, С.И. БАБКИН, канд. техн. наук,
И.В. КОРЫТЦЕВ, канд. техн. наук, О.В. ЗУБКОВ, канд. техн. наук, М.А АНОХИН

ИНФОРМАЦИОННЫЕ ХАРАКТЕРИСТИКИ ЗВУКОВОГО ИЗЛУЧЕНИЯ МАЛЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Введение

В настоящее время количество сфер применения малых беспилотных летательных аппаратов (БПЛА) стремительно растет. Среди сравнительно новых потребительских рынков БПЛА можно отметить лесное, сельское и дорожное хозяйство, энергетику и связь, добычу и транспортировку нефти и газа, безопасность и охрану окружающей среды и многие другие. Многие малые БПЛА стали доступными для обычных пользователей, причем их оснащение достаточно сложное и включает фото- и видеокамеры, систему автопилота и навигации, что делает управление такими БПЛА достаточно простым.

Повсеместное использование малых БПЛА помимо, несомненно, позитивных сторон породило ряд проблем, связанных с неадекватным поведением некоторых владельцев БПЛА, несанкционированным мониторингом объектов и территорий государственной важности, участившимися случаями вторжения в личную жизнь и т.д. В ряде перечисленных случаев актуальным становится обнаружение БПЛА в воздухе, что может быть осуществлено средствами активной и пассивной радиолокации, тепловой локации, системами видеонаблюдения. В случае БПЛА, имеющих малые размеры, маломощные электродвигатели, которые иногда не имеют управления по радиоканалу, применение указанных методов имеет ряд существенных сложностей и ограничений.

Одним из направлений в обнаружении БПЛА являются акустические наблюдения [1 – 4]. Шум, создаваемый силовой установкой БПЛА и воздушным винтом, является существенным демаскирующим признаком. Создание и совершенствование методов обнаружения, пеленгации и распознавания малых БПЛА путем приема и обработки звуковых сигналов является актуальной задачей.

Методы обработки звуковых сигналов, описанные в литературе, в основном направлены на распознавание звуковых команд в системах управления, что позволяет максимально упростить работу с системой, ускорить и облегчить доступ к данным в информационных базах. Примером использования могут служить такие разработки, как: “VoiceCom SDK”, система “Voice Navigator” или система управления бытовым оборудованием “Труффальдино”. Такие системы не только вносят комфорт и разнообразие в нашу жизнь, но и облегчают жизнь людей с ограниченными возможностями движения. Эти методы базируются на оценках параметров речевых звуков, используют линейное предсказывающее кодирование (LPC), мел-частотные коэффициенты кепстров (MFCC), перцептуальное линейное предсказание (PLP), но мало пригодны для обнаружения малых летательных аппаратов по их акустическим шумам.

Пассивные содары обладают небольшим радиусом действия, поэтому процесс обработки сигналов должен укладываться в минимальный промежуток времени, а система обработки должна распознавать БПЛА на фоне акустических шумов и помех.

При распознавании объектов наиболее важной и проблемной задачей является выделение признаков. Тяжело добиться надежной работы алгоритма системы распознавания при отсутствии количества корректных признаков, достаточного для классификации объектов и их распознавания. Выбор признаков влияет на процесс построения алгоритма распознавания, а также на производительность всей системы и качество распознавания.

1. Результаты исследований характеристик звукового излучения некоторых малых БПЛА и их анализ

Экспериментальная установка для исследований состояла из измерительного конденсаторного микрофона Superlux ECM-999, установленного в фокусе параболического отражателя диаметром 0,6 м. Выход микрофона подключался по симметричному аудиоинтерфейсу XLR ко входу внешней звуковой карты Behringer U-Phoria UM2. Звуковой сигнал оцифровывался с частотой дискретизации 48 кГц и разрядностью 24 бита. Эксперименты проводились в условиях города, во внутреннем дворе Харьковского национального университета радиоэлектроники. Отношение сигнал/шум в обрабатываемых записях составило около 20 дБ. Исследованы акустические излучения квадрокоптера DJI Phantom 2 и моноплана Skywalker Falcon 1340 mm EPO Flying Wing.

Акустические измерения для квадрокоптера были проведены в режимах подъема над акустической антенной, барражирования на высоте 50 м и последующей посадки. На рис. 1 показана временная реализация записи звукового сигнала квадрокоптера длительностью 20 мс на этапе барражирования, а на рис. 2 – нормированная автокорреляционная функция (АКФ) для данной реализации. Звуковой сигнал квадрокоптера имеет периодический характер, основной период для винта с N лопастями при угловой скорости его вращения Ω определяется выражением $T = 2\pi / N\Omega$ [5].

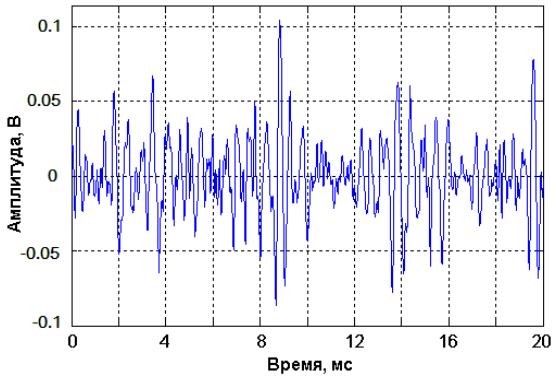


Рис. 1

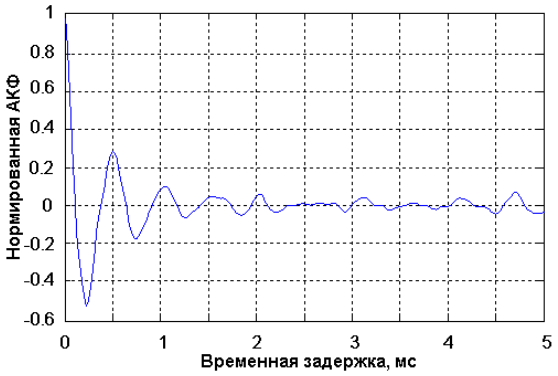


Рис. 2

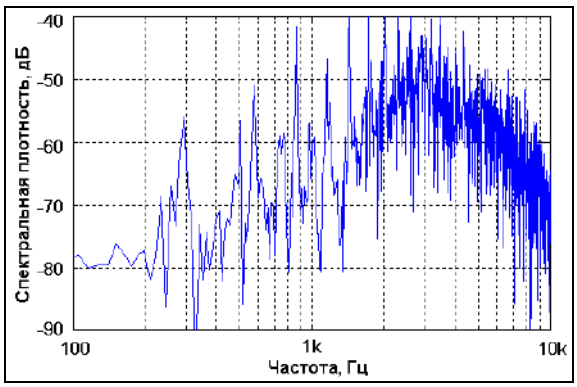


Рис. 3

На рис. 3 показан амплитудный спектр звукового сигнала квадрокоптера, полученный путем БПФ по выборке 8192 отсчета без накопления. Спектр сигнала содержит широкополосную шумовую составляющую (явно выраженный пологий максимум) и многокомпонентную гармоническую структуру, частоты гармонических составляющих являются кратными числами. Анализ большого числа реализаций показывает, что уверенно обнаруживаются, даже при наличии временного накопления, гармоники с частотами до 10 кГц. Амплитуды и фазы гармоник являются случайными и при отсутствии движения квадрокоптера. Это объясняется некоторым различием режимов работы двигателей в процессе компенсации автоматикой БПЛА ветрового воздействия. Данный фактор также приводит к некоторому расширению спектральных линий.

Динамика работы системы компенсации ветровых возмущений квадрокоптера хорошо заметна в частотно-временной области. На рис. 4 показана спектрограмма акустического сигнала для реализации длительностью 15 с. В режиме активного парирования ветра спектральные максимумы разделяются, их количество соответствует числу двигателей аппарата. Последние 2 с на спектрограмме соответствуют этапу посадки квадрокоптера с уменьшением частоты вращения двигателей.

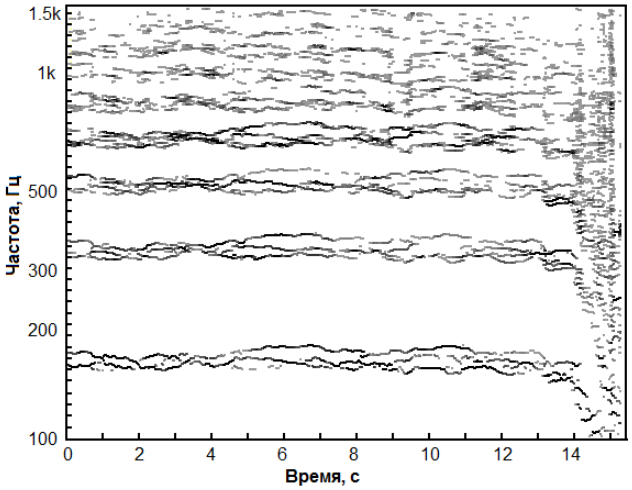


Рис. 4

На рис. 5, 6 показаны псевдофазовые портреты двух реализаций звукового сигнала квадрокоптера. Они показывают зависимость последующего значения сигнала $Y = s(t + \Delta)$ от предыдущего $X = s(t)$. Временной сдвиг Δ выбирался после анализа АКФ и соответствовал ее основному периоду. Очевидно, что полученные псевдофазовые портреты не отвечают представлениям о классических аттракторах, поэтому для выявления их природы необходим дополнительный анализ.

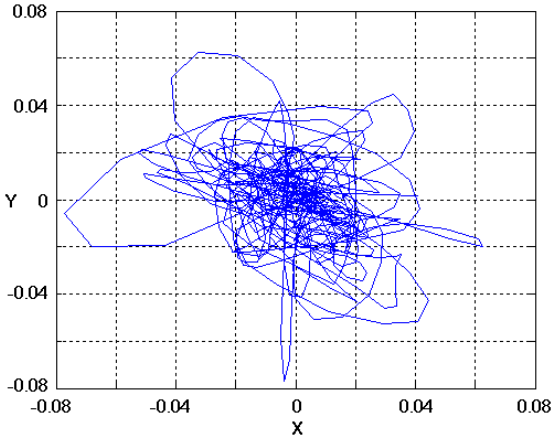


Рис. 5

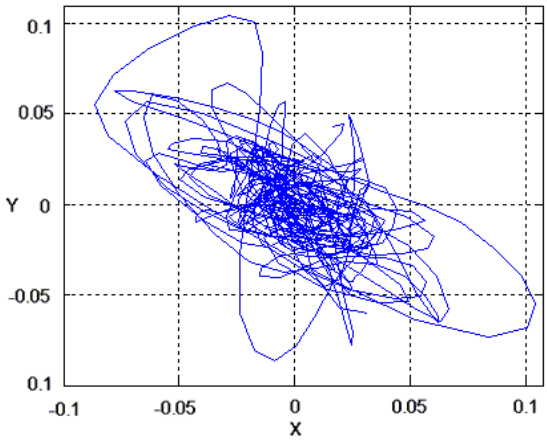


Рис. 6

Измерения для моноплана проводились в режиме пролета над акустической антенной на высоте около 20 м. На рис. 7 показана временная реализация записи звукового сигнала моноплана, а на рис. 8 – ее нормированная АКФ.

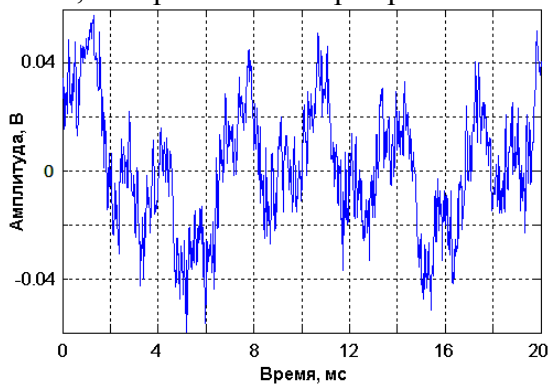


Рис. 7

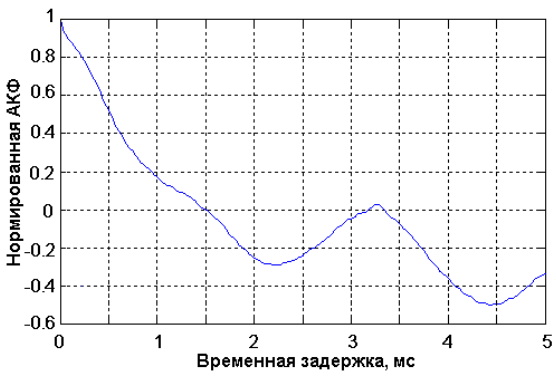


Рис. 8

В данной записи, в отличие от записей звукового сигнала квадрокоптера, присутствует заметная низкочастотная составляющая на частотах до 200 – 250 Гц. Появление этой составляющей вызвано "задуванием" ветра в микрофон измерительной установки. Это свидетельствует о необходимости применения специальной ветрозащиты микрофона и низкочастотной фильтрации при построении систем обнаружения БПЛА.

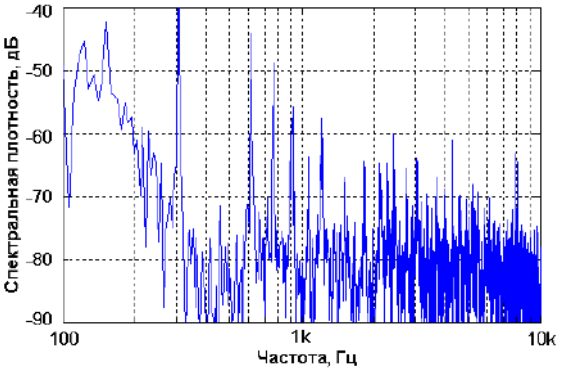


Рис. 9

На рис. 10 показана спектрограмма звукового сигнала моноплана для реализации длительностью 4,5 с.

Данная запись получена для случая пикирования в точку над акустической антенной на высоте около 10 м (временной интервал 1,8 – 2,4 с), последующим выравниванием и переходом в горизонтальный полет. Поскольку в данном сеансе режим двигателя оставался неизменным, синхронное изменение частот гармоник звукового сигнала моноплана вызвано эффектом Доплера при пролете над акустической антенной. При акустическом наблюдении моноплана под малыми углами к направлению движения структура спек тра изменяется медленно, что дает возможность применять временное накопление на длительных интервалах.

Спектр звукового сигнала моноплана (рис. 9) также имеет в своем составе большое количество гармоник вплоть до частот 8 – 10 кГц. Спектральные линии, в отличие от квадрокоптера, узкие, что объясняется наличием одного двигателя в силовой установке. Соотношение между амплитудами гармоник менее изменчиво во времени, чем в случае квадрокоптера, а изменение частоты обусловлено совместным действием двух факторов – эффектом Доплера и изменением режима двигателя.

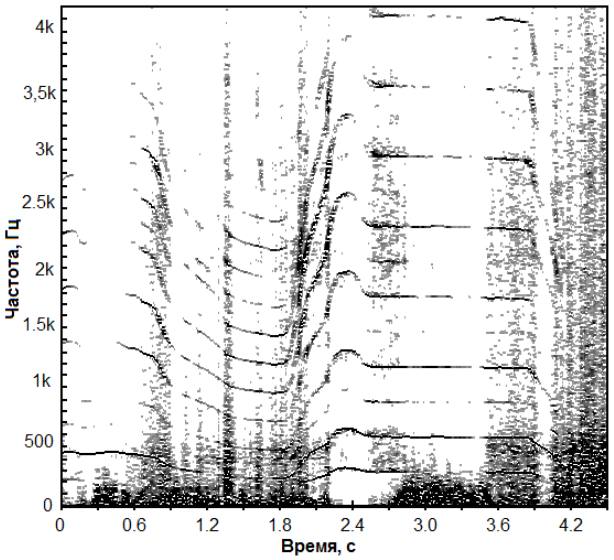


Рис. 10

2. Обнаружение БПЛА на фоне акустических шумов и помех

2.1. Построение первичных признаков звукового образа БПЛА

Принимаемые пассивным содаром звуковые колебания БПЛА преобразуются в электрический сигнал, представляющий собой реализацию широкополосного случайного процесса, описание которого может быть дано энергетическим спектром. Поэтому информационными признаками звукового образа БПЛА могут служить оценки спектральных коэффициентов, определяемые по дискретной реализации S, содержащей N отсчетов, согласно выражению [6]

$$\hat{G}_s(n\Delta f) = \frac{2\Delta t}{N}\left|\sum_{i=0}^{N-1} S(i\Delta t)exp\{-j2\pi in/N\}\right|^2 \qquad (1)$$

где $S(i\Delta t)$ – отсчеты шумовой реализации; $\Delta f = \frac{1}{N\Delta t}; \quad n = 0, 1, 2, \ldots, \frac{N}{2}.$

Сглаживание полученного ансамбля спектральных коэффициентов прямоугольной весовой функцией обеспечивает состоятельность оценок и физически дает характерную структуру спектра, содержащую явно выраженные гармонические составляющие – шум пропеллера (пропеллеров), а также в середине интервала звуковых частот плавно нарастающую и спадающую шумовую составляющую – шум всего летательного аппарата. Эта структура отличает звуковой образ одного БПЛА от другого и от звуковых образов других объектов, естественного акустического шума и помех.

Ортогонализация спектров [7] позволяет выбрать во вторичном пространстве более информативные признаки при меньшем их количестве для описания звукового образа, что повысит оперативность системы.

2.2. Формирование вторичных информативных признаков

Обычно спектральному анализу подвергаются выборки звукового сигнала, в которых количество отсчетов определяется степенью числа два. Соответственно определится и набор спектральных коэффициентов, который можно записать для выборки в виде вектора

$$\vec{F} = (F_1, F_2, \ldots, F_k, \ldots, F_n)^T,$$

где T – символ транспонирования, F_k соответствует k-му сглаженному спектральному коэффициенту (1); n – размерность вектора.

Выборочная матрица F спектральных коэффициентов будет выглядеть следующим образом для каждого звукового образа

$$F = \begin{Vmatrix} F_{11} & F_{12} & \cdots & F_{1m} \\ F_{21} & F_{22} & \cdots & F_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ F_{n1} & F_{n2} & \cdots & F_{nm} \end{Vmatrix}, \qquad (2)$$

где m – число отдельно наблюдаемых спектральных векторов.

Переход ко вторичным информационным признакам осуществляется путем построения ковариационной матрицы спектральных коэффициентов и ее диагонализации. Так, ковариационная матрица получается в виде усредненного произведения матрицы (2) и ее транспонированной

$$K = \frac{1}{m} F F^T,$$

при этом предполагается, что среднее значение каждой составляющей уже исключено.

Используя ортогональную матрицу U, столбцы которой являются собственными векторами матрицы K, получаем диагонализацию ковариационной матрицы [8]

$$U^T K U = \begin{Vmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{Vmatrix} \qquad (3)$$

На главной диагонали матрицы находятся собственные числа, а все остальные элементы равны нулю. Собственные числа матрицы (3) и собственные векторы матрицы K могут быть использованы в качестве эффективных вторичных информативных признаков при распознавании звуковых образов.

2.3. Правило принятия решений

Для принятия решений о принадлежности входного звукового образа, представленного усеченной матрицей собственных векторов, соответствующих большим собственным чис-

лам, было разработано решающее правило, базирующееся на критерии подобия Дайса [9]. Векторное представление информационных признаков позволяет рассчитать коэффициенты подобия Дайса. При этом некоторая избыточность набора признаков, используемого для расчета значения коэффициента подобия, позволяет более эффективно классифицировать образы, поскольку использование малого количества признаков приводит к неправильному определению подобия пары образов. Для расчета коэффициента подобия (D) используется формула [10]

$$D(A,B)=\frac{2\times\sum_{i=1}^{n}a_i b_i}{\sum_{i=1}^{n}a_i^2+\sum_{i=1}^{n}b_i^2}, \qquad (4)$$

где a_i – сличаемые координаты собственного вектора ковариационной матрицы входного звукового образа; b_i – координаты соответствующего собственного вектора из коллекции; A, B – собственные векторы усеченной ковариационной матрицы, столбцы которой соответствуют наибольшим собственным числам, для входного звукового образа и образа из коллекции.

После проведенных расчетов набор признаков, поступивший на вход системы, соответствует некоторому классу, если среднее значение коэффициента подобия по всем парам сличаемых векторов больше определенной пороговой величины. Улучшение качества распознавания при использовании коэффициентов подобия обеспечивается получением больших значений подобия для наиболее соответствующих образов, поскольку в расчете не учитываются малозначимые элементы набора признаков.

Выводы

Экспериментальное исследование звуковых сигналов квадрокоптера и моноплана показало, что их спектры имеют ярко выраженные гармонические составляющие с частотами, кратными частоте вращения винта.

Гармонические составляющие звукового сигнала квадрокоптера шире, чем у моноплана, что объясняется некоторым различием режимов работы двигателей в процессе полета или при работе системы компенсации ветровых возмущений.

При большом различии режимов двигателей квадрокоптера спектральные максимумы разделяются на несколько, что может быть одним из признаков для классификации БПЛА.

В звуковых сигналах исследованных БПЛА, при наличии накопления спектров, уверенно наблюдаются гармоники с частотами до 8 – 10 кГц.

При акустическом наблюдении БПЛА самолетного типа под малыми углами к направлению движения структура спектра изменяется незначительно, что дает возможность применять временное накопление на длительных интервалах.

Проведенные теоретические исследования позволяют разработать модуль формирования коллекции звуковых образов БПЛА и модуль, реализующий правило принятия решений. Полученные данные могут быть использованы и в других системах, требующих оперативного распознавания объектов.

Список литературы: 1. *Zelnio, A.M.* Detection of small aircraft using an acoustic array. Thesis. B.S. / A.M. Zelnio. – Electrical Engineering, Wright State University. – 2007. – 55 p. 2. *Pham, T.* TTCP AG-6: Acousting detection and tracking of UAVs / T.Pham, N.Srour // U.S. Army Research Laboratory. Proc. of SPIE.- 2004. – Vol. 54. – Pp. 24–29. 3. *Sadasivan, S.* Acoustis siqnature of an unmanned air vehicle – exploitation for aircraft localisation and parameter estimation / S.Sadasivan, M.Gurubasavaraj, S.R. Sekar // Eronautical DEF SCI J. – 2001. – Vol. 51, № 3. – Pp. 279–283. 4. *Kartashov V.M., Babkin S.I., Tolstykh E.G., Lepeha N.G.* Systematic errors in measurement of meteorological variables in correlation processing radioacoustic sounding system signals // Telecommunications and Radio Engineering (English translation of Electrosvyaz and Radiotekhika). – 2016. – V.75 (9). – Pp. 835-843. 5. *Александров, В.Л.* Воз-

душные винты. – М. : Гос. изд-во оборонной промышленности. – 1951. – С. 376–377. 6. *Грибанов, Ю.И., Мальков, В.Л.* Спектральный анализ случайных процессов. – М. : Энергия. – 1974. – 239 с. 7. *Безрук, В.М., Певцов, Г.В.* Теоретические основы проектирования систем распознавания сигналов для автоматизированного радиоконтроля. – Харьков : Коллегиум, 2007. – 430с. 8. *Беллман, Р. Э.* Введение в теорию матриц. – М. : Наука, 1969. – 368с. 9. *Sung-Huyk, C.* Comprehensive Survey on Distance/Similarity Measures between Probability Density Functions // International Journal of Mathematical Models and Methods in Applied Science. – 2007. – Vol.1. – Issue 4. – Pp. 300-307. 10. *Anokhin, M., Koryttse, I.* Decision-making rule efficiency estimation with applying similarity metrics. – Lublin-Rzeszow: ECONTTECHMOD. – 2015. – Vol.4. – No3. – С. 73-78.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 14.11.2017

УДК 621.391

ХАССАН МОХАМЕД МУХИ-АЛДИН, Е.Б. ТКАЧЕВА, канд. техн. наук

АДАПТИВНЫЙ АЛГОРИТМ ПЕРЕРАСПРЕДЕЛЕНИЯ СЕТЕВЫХ РЕСУРСОВ В СЕТЯХ С ПОДДЕРЖКОЙ ТЕХНОЛОГИИ NFV

Введение

Стремительно возрастающие потребности пользователей мультисервисных сетей к качеству и разновидностям предоставляемых сервисов влекут за собой необходимость расширения спектра и способов предоставления сервисов со стороны сервис-провайдеров. Широкую популярность приобретают комплексные сервисы, которые подразумевают «бесшовное» совместное функционирование множества атомарных сервисов с целью максимального удовлетворения потребностей пользователей к качеству обслуживания (Quality of Services, QoS). Предоставление подобных сервисов сопряжено с процессами оркестровки, хореографии и последующего мониторинга [1] высокую эффективность которых достаточно трудно обеспечить в традиционных мультисервисных сетях. Одним из решений, позволяющих повысить эффективность процессов управления и предоставления комплексных сервисов, является технология виртуализации сетевых функций (Network Function Virtualization, NFV) [2, 3].

В основе NFV лежит возможность виртуализации множества сервисов, в том числе и тех, которые в традиционных мультисервисных сетях поддерживаются лишь аппаратно. По мере роста популярности NFV возрастает и сложность систем управления ими. Так, некорректное распределение ресурсов в NFV может повлечь за собой нерациональное использование сетевых ресурсов:

- недостаточную загруженность в тех зонах сети, где интенсивность запросов к сервисам невелика, что приводит к неоправданному увеличению финансовых затрат на поддержку как виртуальной среды, так и физической сети, поверх которых она реализована;
- потенциальную перегрузку в тех зонах сети, где интенсивность запросов к сервисам велика, что приводит к возникновению сбоев и отказов в доступе, а следовательно, снижение надежности влечет за собой наложение штрафных санкций.

Для устранения приведенных недостатков применяются механизмы динамического перераспределения сетевых ресурсов или миграции виртуальных узлов. Однако при разработке подобных механизмов возникает ряд трудностей, связанных с неоправданно высокой стоимостью точного расчета интенсивности нагрузки, распределения запросов к виртуальным сетевым ресурсам и уровня популярности предоставляемых сервисов [4, 5].

Множество работ, посвященных разработке методов перераспределения сетевых ресурсов, основано на распределении виртуальных ресурсов, где в качестве целевой функции выступают: минимизация пропускной способности каналов связи [6], повышение уровня доступности путем резервирования ресурсов [7] или дорогостоящей самоорганизации сети [8]. Применение подходов [6 – 8] позволяет достаточно хорошо адаптироваться к перегрузкам сети, однако не позволяет оценить стоимость данной адаптации – стоимость перераспределения ресурсов, что в ряде случаев приводит к неэффективному использованию ресурсов. Таким образом, разработка алгоритма, позволяющего реактивно реагировать на ухудшения качества сервисов в мультисервисных сетях с поддержкой технологии NFV, а также учитывать стоимость процесса перераспределения сетевых ресурсов, является актуальной задачей.

Алгоритм перераспределения сетевых ресурсов, основанный на учете стоимости

В соответствии с ETSI [9, 10], архитектура мультисервисной сети с поддержкой функций виртуализации состоит из трех ключевых компонентов: физических ресурсов, виртуальных ресурсов (узлов) и платформы управления и оркестровки сервисов (NFV MANO).

Структурная схема архитектуры мультисервисной сети с поддержкой функций виртуализации приведена на рис. 1.

За корректное взаимодействие между физическими и виртуальными компонентами сетевой инфраструктуры отвечает компонент MANO.

Физические ресурсы NFVI включают в себя серверное оборудование, оборудование коммутации и маршрутизации, системы хранения данных и каналы связи. Слаженное взаимодействие данных компонентов обеспечивает корректную передачу данных от оконечного пользователя к вычислительным элементам, и наоборот.

Уровень виртуализации представляет собой множество абстракций: виртуальные машины с разными операционными системами (ОС) и приложениями и центры хранения данных. Именно они обеспечивают формирование и предоставление полного спектра услуг оконечным пользователям.

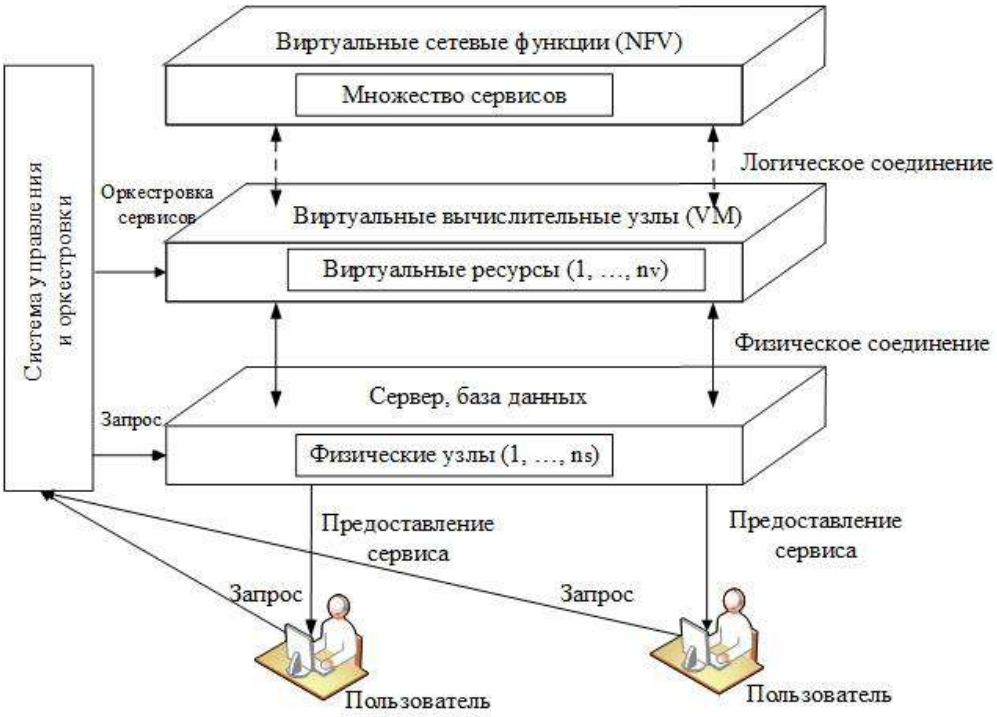


Рис. 1

В процессе предоставления сервисов может потребоваться выделение дополнительных ресурсов – как виртуальных, так и физических. При этом нехватка физических ресурсов приводит к ограничению виртуальных ресурсов и, как следствие, деградации качества сервисов, запущенных на виртуальных узлах. С целью поддержки требуемого уровня качества применяются механизмы миграции [4 – 8], нацеленные на повышение уровня производительности путем переноса услуги на наименее загруженный физический узел сети [7], минимизацию требуемой пропускной способности каналов [6] во время миграции, повышение уровня доступности путем резервирования ресурсов [8]. Существующие алгоритмы перераспределения сетевых ресурсов обладают общим существенным недостатком – принятие управляющего решения на основе статистических данных, что не позволяет оценить текущее взаимодействие сетевых ресурсов.

С целью описания взаимодействия компонентов сети при разработке алгоритма миграции предложено использовать модельный подход [11]. Физическая инфраструктура мультисервисной сети представлена ориентированным графом вида

$$G_s = (N_s, E_s), \tag{1}$$

где N_s – множество физических узлов сети: $\{n_{s1}, n_{s2}, n_{s3}, ... \in N_s\}$, E_s – множество дуг, обеспечивающих связи между узлами $\{l_{s1}, l_{s2}, l_{s3}, ... \in E_s\}$.

Виртуальная сетевая архитектура, накладываемая на физические сетевые ресурсы по аналогии с описанием физической инфраструктуры, также может быть представлена ориентированным графом (рис. 1)

$$G_v = (N_v, E_v), \tag{2}$$

где N_v – множество виртуальных узлов, реализующих требуемые сервисы: $\{n_{v1}, n_{v2}, n_{v3}, ... \in N_v\}$, E_v – множество дуг, отображающих взаимодействие между узлами, $\{l_{v1}, l_{v2}, l_{v3}, ... \in E_v\}$. Каждый виртуальный узел $n_{vs}, \{v \in N_v\}$ характеризуется уровнем производительности, $a_{n_v}(t)$, а дуга – требуемой пропускной способностью, $a_{l_v}(t)$.

В соответствии с рекомендациями RFC 7149 [12], IETF P1903.3 [13], ETSI GS NFV 002 [14] с целью комплексной оценки показателей качества обслуживания в мультисервисных сетях с поддержкой NFV предложено проводить анализ и последующую оценку следующих показателей:

- стоимость предоставления сервиса *c(s)*;
- время отклика в процессе предоставления сервиса *t(s)*;
- надежность *r(s)*;
- доступность *a(s)*.

В целом, значение показателей *t(s), r(s), a(s)* может быть охарактеризовано комплексным показателем, значение которого зависит как от производительности физического и виртуального узлов, а также пропускных способностей физического и виртуального каналов связи, задействованных в предоставлении услуги:

$$\begin{gathered} p_s(t) = p_{n_s}(t) + p_{v_s}(t); \\ Th_s(t) = \min(Th_{l_s}(t), Th_{l_v}(t)), \end{gathered} \tag{3}$$

где $p_{n_s}(t)$ – производительность физического узла в момент времени t; $p_{v_s}(t)$ – производительность виртуального узла в момент времени t. Производительность виртуального узла всегда ограничена производительностью физического узла, на котором он развернут: $p_{v_s}(t) < p_{n_s}(t)$; $Th_{l_s}(t)$ – доступная пропускная способность физических канальных ресурсов в момент времени t; $Th_{l_v}(t)$ – доступная пропускная способность виртуальных канальных ресурсов в момент времени t, пропускная способность виртуального канала связи не превышает пропускную способность $Th_{l_s}(t)$: $Th_{l_v}(t) < Th_{l_s}(t)$,

В случае, если физической узел не способен обеспечить производительность, необходимую для эффективного функционирования виртуальных ресурсов, а следовательно, и предоставления сервисов с требуемым уровнем качества, в сетях с поддержкой виртуализации сетевых функций активируются механизмы перераспределения ресурсов в сети.

Перераспределение ресурсов осуществляется за счет миграции виртуального узла на другой, менее загруженный, физический узел сети. Предлагаемый алгоритм миграции наряду с анализом текущей производительности физических узлов позволяет также учитывать стоимость миграции. Результатом функционирования алгоритма является набор физических узлов с требуемым уровнем производительности, стоимость миграции на которые является наименьшей.

Целевая функция QO может быть представлена следующим образом:

$$Q(p_s, C_{tot}(n_v)) \to \min_{CP_\alpha}, \quad (4)$$

где p_s – суммарная производительность, c_s – стоимость миграции, CP_α – политика управления сетевой нагрузкой.

В данном случае задачу оптимизации можно свести к задаче поиска минимального значения суммарной стоимости перераспределения сетевых ресурсов $\min(C_{tot}(n_v))$

Суммарная стоимость перераспределения ресурсов включает в себя следующие составляющие:

- стоимость «разворачивания» узла на новом физическом устройстве, которая включает стоимость простоя сервисов во время выбора альтернативных физических узлов и подготовку к разворачиванию нового виртуального узла, $C_{reloc}(n_v)$;
- стоимость поддержки соединения между альтернативным физическим узлом и деградирующим узлом, которая включает выделение требуемой пропускной способности канала и поддержку требуемого уровня производительности альтернативного физического узла, $C_{mig}(n_v)$ и может быть задана следующим выражением:

$$C_{tot}(n_v) = C_{suspend}(n_v) + p_{n_s^r}(t) * C(M_{N_v^r}(n^r)) + \sum_{l_s} \sum_{l_v \in M_{L_v^r}} Th_{l_v^r}(t) * C(M_{L_v^r}(l^r)), \quad (5)$$

где $p_{n_s^r}(t)$ – альтернативный физический узел, соответствующий требованиям, выдвигаемым к производительности, $C(M_{N_v^r}(n^r)$ – стоимость размещения виртуального узла на выбранном физическом узле, $Th_{l_v^r}$ – пропускная способность канала передачи данных между выбранным физическим узлом и деградирующим физическим узлом, на котором размещен виртуальный узел; $C(M_{L_v^r}(l^r)$ – стоимость миграции виртуального узла.

Минимально требуемая пропускная способность, выделяемая для переноса виртуального узла на альтернативный физический узел, может быть определена следующим образом:

$$\min Th_{l_v^r} = \frac{|n_v|_{l_s \in p_{mig}(n_v^r)}}{\max T_{QoS}}, \quad (6)$$

где $|n_v|_{l_s \in p_{mig}(n_v^r)}$ – размер переносимого виртуального узла (Мб), $\max T_{QoS}$ – максимальное время доступа к услуги без наложения штрафных санкций.

В этом случае стоимость миграции включает в себя стоимость выделения / резервирования пропускной способности, необходимой для миграции:

$$C_{mig}(n_v) = C(l_s) * \sum_{l_s \in p_{mig}(n_v^r)} \min Th_{l_v^r}, \quad (7)$$

где $l_s \in p_{mig}(n_v^r)$ – маршрут, используемый для миграции виртуального узла на альтернативный физический узел.

Суммарная стоимость миграции включает в себя стоимость перераспределения ресурсов и непосредственно стоимость миграции:

$$C_{tot}(n_v) = C_{reloc}(n_v) + C_{mig}(n_v). \quad (8)$$

Ключевой задачей предлагаемого алгоритма перераспределения ресурсов является поиск такого физическоо узла и маршрута $l_s \in p_{mig}(n_v^r)$ миграции, при котором суммарная составляющая стоимости перераспределения сводятся к минимуму $C_{tot}(n_v) \to \min$

Перераспределение ресурсов с целью обеспечения минимальной общей стоимости предложено выполнять в несколько этапов:

- определение набора виртуальных узлов, миграция которых является необходимой. Как отмечено ранее, в качестве таких узлов выступают узлы, нагрузка на которые постоянно увеличивается, а производительность, с увеличением нагрузки, уменьшается (как правило, наблюдается снижение физического узла);
- определение набора физических узлов, наиболее подходящих для перемещения, которые размещены в одной зоне с деградирующим сервисом. В качестве таких узлов выступают наиболее терпимые к сбоям и перегрузкам;
- формирование маршрутов, позволяющих обеспечить наименьшую стоимость и оконечный выбор узлов для миграции. алгоритм должен эффективно отображать узлы и ссылки для достижения минимальной цели перераспределения и миграции;
- расчет $C_{reloc}(n_v)$ и $C_{mig}(n_v)$.

Псевдокод, описывающий поведение разработанного алгоритма, может быть представлен следующим образом:

```
Reallocate(nv, min(Ctot(nv)))
ReallocationResult←failure
Remap Ctot(nv) ←∞
Search neartnrv
if neartnv is less than required then
  for all ns ∈ near nv(degrad)
     do map nv in ns
     for all lv ∈ Snv do
     re-map virtual node to physical node
   end for
if Ns mapping succeeds then
ReallocationResult success
if Creloc(Ns) < Creloc(Ns+i)  then
    do route nv(degrad) in Ns
    for all lv ∈ Es ∩ Ev do
       do route nv in ns
       for all lv ∈ Snv do
route virtual link ls onto a substrate path α using shortest path algorithm
       end if
      end if
     end if
end for
if ReallocationResult = Success then
Add Creloc(nv) + Cmig(nv) to Ctot(nv)
end if
end if
return ReallocationResult
```

Оценка эффективности предлагаемого метода динамического распределения пропускной способности каналов связи

Для оценки эффективности предлагаемого алгоритма балансировки нагрузки для сетей с поддержкой технологии NFV использовался сетевой эмулятор mininet [15]. Топология экспериментального фрагмента сети приведена на рис. 2.

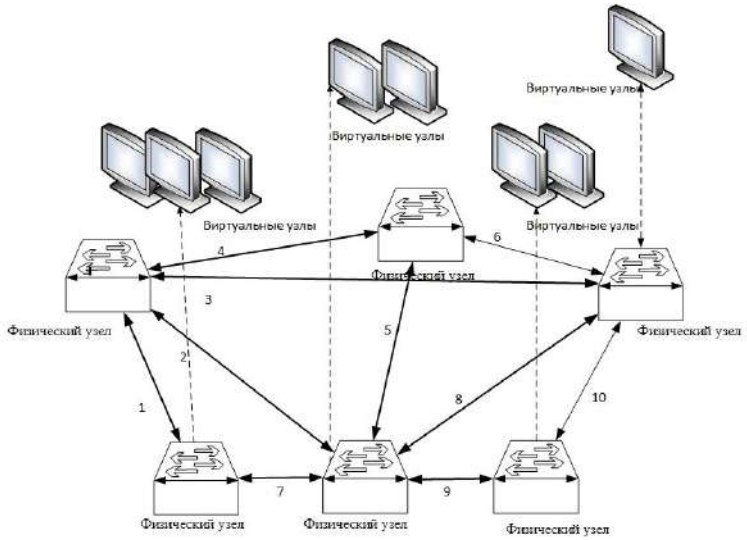


Рис. 2

В процессе эксперимента применялись алгоритмы перераспределения виртуальных ресурсов сети, которые имеют достаточный уровень апробаций: RSforEVN [8] и DVNMA_NS [16], а также предложенный в работе алгоритм.

Для оценки результатов эксперимента предложено использовать следующие метрики:

- стоимость «разворачивания» узла на новом физическом устройстве $C_{reloc}(n_v)$;
- стоимость миграции $C_{mig}(n_v)$.

Входными данными в процессе проведения эксперимента выступали:

- пороговое значение производительности физического узла – 80 %;
- пороговое значение пропускной способности – 1,2 Мб/с;
- пороговое значение времени отклика – 50 мс;
- объем данных при миграции – 780 Мб.

Данные, полученные в результате эксперимента, приведены в таблице.

Результирующее значение стоимости перераспределения ресурсов

Стоимость «разворачивания» узла на новом физическом устройстве $C_{reloc}(n_v)$		
RSforEVN	DVNMA_NS	Разработанный алгоритм
77	450	97
Стоимость миграции $C_{mig}(n_v)$		
RSforEVN	DVNMA_NS	Разработанный алгоритм
126	457	115

Как показывают результаты эксперимента, стоимость планового перераспределения ресурсов разработанного алгоритма значительно не уступает стоимости RSforEVN, но в 4,5 раза меньше стоимости DVNMA_NS, а при оценке стоимости миграции – является минимальной. Основным преимуществом разработанного алгоритм является выбор ближайших альтернативных физических узлов, производительность которых не превышает заданную границу, что позволяет существенно сократить стоимость миграции.

Выводы

В работе предложен алгоритм перераспределения сетевых ресурсов в мультисервисных сетях с поддержкой технологии NFV, позволяющий учитывать стоимость процесса перерас-

пределения сетевых ресурсов, основной особенностью которого является формирование множества альтернативных физических узлов, размещенных в одной или ближайшей зоне с деградирующим сервисом. Приведена математическая модель оценки суммарной стоимости перераспределения (5) – (8). По результатам математического моделирования проведен эксперимент, который показал, что выигрыш суммарной стоимости от использования разработанного алгоритма по сравнению с алгоритмом DVNMA_NS возрастает в 4,5 раза.

Список литературы. 1. *Agushaka, J. O.* Effect of Weighting Scheme to QoS Properties in Web Service Discovery/Agushaka J.O., Lawal M. M., Bagiwa, A. M. and Abdullahi B. F // International Journal of Computer Science and Information Security. – Vol. 7. – No. 3 March 2010. – P.92-100. 2. *ETSI* Industry Specification Group (ISG). NFV, ETSI GS NFV 002 V1.2.1: Network Functions Virtualisation (NFV); Architectural Framework [online]. Available at: http://www.etsi.org/deliver/etsigs/NFV/001099/002/01.02.0160/gsNFV002v010201p.pdf, December 2014. 3. *ETSI* Industry Specification Group (ISG). NFV, ETSI GS NFV-MAN 001 V1.1.1: Network Functions Virtualisation (NFV); Management and Orchestration, http://www.etsi.org/deliver/etsigs/NFV-MAN/001099/001/01.01.0160/gsNFV-MAN001v010101p.pdf, December 2014. 4. *Tran, P.N., Timm-Giel, A.* Reconfiguration of virtual network mapping considering service disruption. In: (ICC), 2013. P.160-169. 5. *Lu, J., Turner, M.* Efficient Mapping of Virtual Networks onto a Shared Substrate. Tech. rept. Washington University in St. Louis, Jonathan. 2006. 152 p. 6. *Zhang, S., Sheng, Q. and all*. Virtual Network Embedding with Opportunistic Resource Sharing. Parallel and Distributed Systems // IEEE Transactions. – 2014. – Vol. 25(3). – P. 816–827. 7. *Zhani, M.F., Zhang. Q., Simon, G.* VDC Planner: Dynamic migration-aware Virtual Data Center embedding for clouds // Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. 2014. P.112–118. 8. *Jmila, H., Houidi, I., Zeghlache, D.* RSforVNE: Node Reallocation Algorithm for Virtual Networks Adaptation // 19th IEEE Symposium on Computers and Communications (IEEE ISCC 2014). 9. NFV.Network Operator Perspectives on Industry Progress. Online. Available at: https://portal.etsi.org/NFV/NFV_White_Paper2.pdf 10. Infonetics Research, Inc. SDN and NFV Strategies: Global Service Provider Survey [Электронный ресурс]. 2014. – 39 с. Режим доступа: http://alu.us.neolane.net/res/img/286758382c7e061c52883e873cee02e6.pdf 11. *Поповский, В. В.* Математические основы управления и адаптации в телекоммуникационных системах : ученик / В. В. Поповский, В. Ф. Олейник. – Харьков : СМИТ, 2011. – 362 с. 12. *ITU-T* Recommendation E.802. Series E: Overall network operation, telephone service, service operations and human factors – Framework and methodologies for the determination and application of QoS parameters. Geneva: International Telecommunications Union. – 2007. 13. *P1903.3* – Standard for Self-Organizing Management Protocols of Next Generation Service Overlay Network (NGSON) 14. *GS NFV* 002 Network Functions Virtualisation (NFV); Architectural Framework. 15. *Mininet*: An Instant Virtual Network on your Laptop (or other PC) [Элекронный ресурс] – Режим доступа: http://mininet.org/ 16. *Sun G., Yu H., Anand V.* A cost efficient framework and algorithm for embedding dynamic virtual network requests // *Future Generation Comp. Syst.* – 2013. – Vol. 29(1). – P.1265–1277.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 23.10.2017

УДК 621.38

A.V. OSADCHUK, Doc. Tech. Scien., Prof., V.S. OSADCHUK, Doc. Tech. Scien., Prof., I.A. OSADCHUK, O.O. SELETSKA, PhD in Tech. Scien.

FREQUENCY TRANSDUCER OF GAS CONCENTRATION IN TRANSISTOR STRUCTURE WITH NEGATIVE RESISTANCE

I. INTRODUCTION

One of the promising scientific direction in the creation of gas transducers is the use of reactive properties of semiconductor devices with negative resistance. It allows to convert gas concentration in the frequency output providing high noise stability as well as high accuracy of gas concentration measurements.

Moreover, the transducers with frequency output have both simplicity and versatility inherent in analog devices in addition to accuracy and noise immunity intrinsic in code output transducers [1 – 3]. These transducers have high sensitivity to measuring parameters, smaller overall dimensions and weight, informational, technological and structural compatibility with microelectronic information processing devices. It provides its advantages over existing gas concentration sensors [4 – 6].

The development of a mathematical model, describing the dependence of active and reactive components of the impedance of the structure is needed to study the properties of the frequency transducer gas concentration. This model includes a transfer function, which is a basis for obtaining the sensitivity of transducer. The transfer function in turn depends on active and reactive components of the output impedance of the transducer.

The study is devoted to discussion of these problems.

II. THEORETICAL AND EXPERIMENTAL RESEARCH

The frequency transducer of the gas concentration based on self-sustained oscillator, with MEMS resistive element MiCS 6814, sensitive to concentration of combustible gases, is shown in Fig. 1.

The oscillator of the device is implemented using equivalent capacity of the impedance on such electrodes as collector and drain of bipolar and MOS field-effect transistor VT1 and VT2 respectively [7, 8]. Voltages U1 and U2 provides supply of circuit.

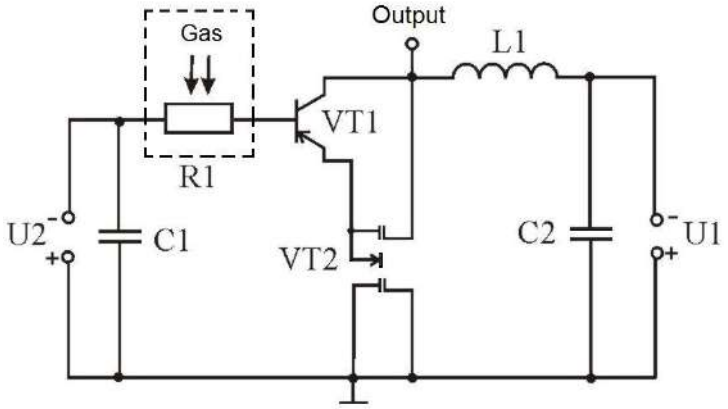


Fig. 1. An elecrtric circuit of frequency transducer of gas concentration

It is necessary that a mathematical model should be developed to study the properties of the frequency transducer of gas concentration. This model enables to obtain the dependencies of active and reactive components of the impedance of the structure on gas concentration, and the analytic expressions for the transfer function and sensitivity [15, 16]. The calculations were performed using the equivalent circuits of bipolar transistor and MOS field-effect transistor for alternating current, which create self-sustained oscillator of the frequency transducer of gas concentration (Fig. 2).

The calculation of the impedance on electrodes collector-drain of bipolar transistor VT1 and MOS field-effect transistor VT2 through equivalent circuit (Fig. 2) is needed to determine main parameters describing the frequency transducer of gas concentration operation [9].

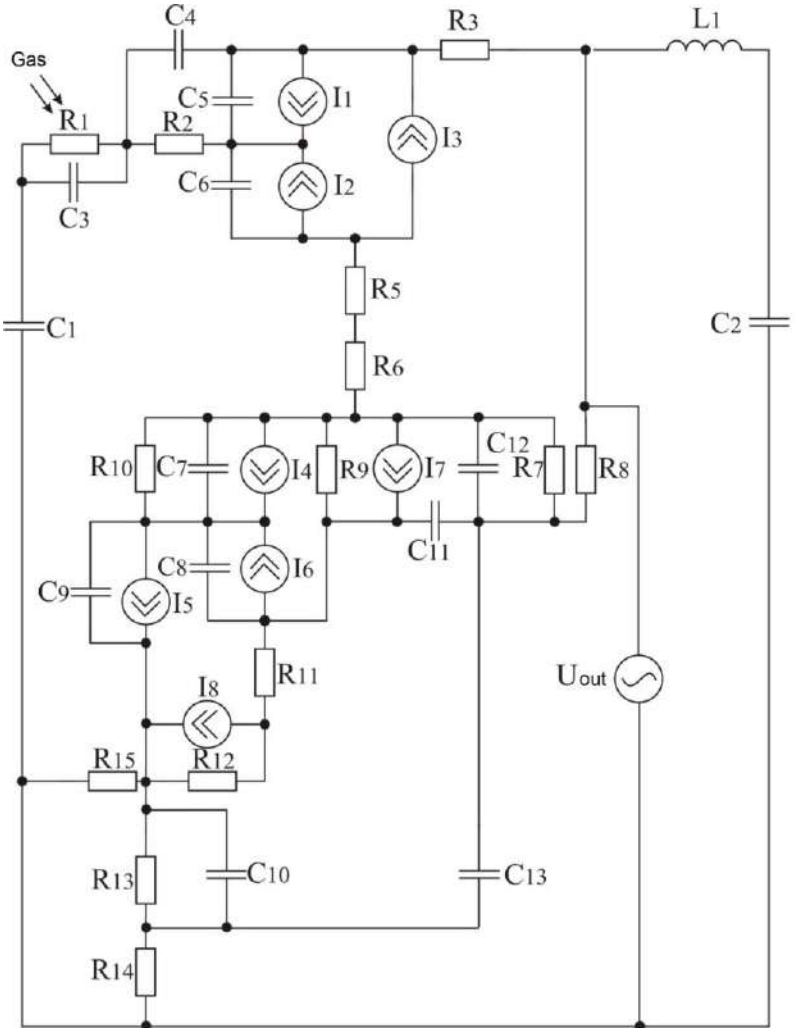


Fig. 2. Equivalent AC circuit of transducer of gas concentration

Fig. 3 shows the equivalent circuit of the frequency transducer of gas concentration for alternating current, transformed into more convenient for calculations.

The current-voltage characteristic curve of the transistor structure which is used for creation of the frequency transducer of gas concentration, has the negative resistance region. The negative resistance compensates losses in the oscillator. It is formed by the equivalent capacity of the electrodes collector-drain of bipolar transistor VT1 and MOS field-effect transistor VT2, and by the external inductance [10-12]. The equivalent circuit (Fig. 2) uses the next symbols: R_1 – resistance of MEMS resistive element MiCS 6814, sensitive to change of concentration of combustible gases; R_2, R_3, R_5 – bulk resistances of emiter, collector and base of bipolar transistor VT1 respectively; R_6, R_{15}, R_8 and R_{14}– bulk resistances of the source, drain, first and second gate of MOS transistor VT2 respectively; R_7 – bulk resistance of gate-source of MOS transistor VT2; R_8 – bulk resistance of gate of MOS transistor VT2; R_9, R_{11} and R_{12} – bulk resistances of drain-source of MOS transistor VT2; R_{10} – resistance of body of MOS transistor VT2; R_{13} – resistance of gate-drain of MOS transistor VT2; C_1 – capacity of capacitor C_1; C_2 – capacity of capacitor C_2; C_3 – capacity of MEMS resistive element MiCS 6814, sensitive to change of concentration of combustible gases; C_4 – capacity beetwen external term of base and collector of bipolar transistor VT1;

C_5, C_6 – capacities of junctions base-collector and base-emiter of transistor VT1 respectively; C_7 – capacity of body-source of MOS transistor VT2; C_8 and C_9 – capacities of body-drain of MOS transistor VT2; C_{10}, $C_{11}$and C_{12} – capacities of gate-drain of MOS transistor VT2; C_{13} – capacity between first and second gates MOS transistors VT2; L_1 – external inductor.

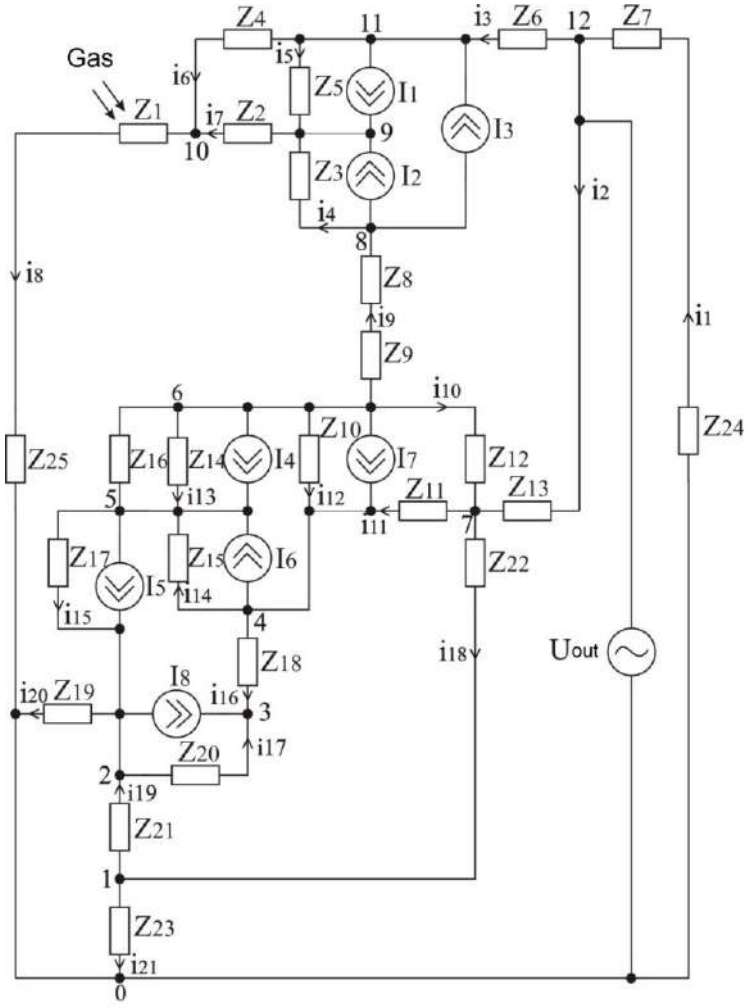


Fig. 3. Transformed equivalent AC circuit of transducer of gas concentration

The following characters are used in the transformed equivalent circuit (Fig. 3):

$$Z_1 = \frac{R_1}{1+\omega^2 R_1^2 C_3^2} - j\frac{R_1^2 \omega C_3}{1+\omega^2 R_1^2 C_3^2};\ Z_2 = R_2;\ Z_3 = -\frac{j}{\omega C_6};\ Z_4 = -\frac{j}{\omega C_4};\ Z_5 = -\frac{j}{\omega C_5}; Z_6 = R_3;$$

$$Z_7 = j\omega L;\ Z_8 = R_5;\ Z_9 = R_6;\ Z_{10} = R_9;\ Z_{11} = -\frac{j}{\omega C_{11}};\ Z_{12} = \frac{R_7}{1+\omega^2 R_7^2 C_{12}^2} - j\frac{R_7^2 \omega C_{12}}{1+\omega^2 R_7^2 C_{12}^2};$$

$$Z_{13} = R_8;\ Z_{14} = -\frac{j}{\omega C_7};\ Z_{15} = -\frac{j}{\omega C_8};\ Z_{16} = R_{10};\ Z_{17} = -\frac{j}{\omega C_9};\ Z_{18} = R_{11};\ Z_{19} = R_{15};$$

$$Z_{20} = R_{12};\ Z_{21} = \frac{R_{13}}{1+\omega^2 R_{13}^2 C_{10}^2} - j\frac{R_{13}^2 \omega C_{10}}{1+\omega^2 R_{13}^2 C_{10}^2};\ Z_{22} = -\frac{j}{\omega C_{13}};\ Z_{23} = R_{14};\ Z_{24} = -\frac{j}{\omega C_2};$$

$$Z_{25} = -\frac{j}{\omega C_1}.$$

In order to receive the components of impedance, we have to solve the Kirchhoff's system of equation for AC created for the equivalent circuit shown in Fig. 3, using circuit node 0 as a basic one (1):

$$\begin{cases} 0 = -\varphi_1(y_{18} + y_{19} - y_{21}) - \varphi_2 y_{19} + \varphi_7 y_{18}; \\ I_8 - I_5 = \varphi_1 y_{19} - \varphi_2(y_{19} + y_{20} + y_{17} + y_{15}) + \varphi_3 y_{17} + \varphi_5 y_{15}; \\ -I_8 = \varphi_2 y_{17} + \varphi_3(y_{16} - y_{17}) + \varphi_4 y_{16}; \\ I_6 - I_1 = \varphi_2 y_{16} - \varphi_4(y_{16} + y_{14} + y_{12} + y_{11}) + \varphi_5 y_{14} + \varphi_6 y_{12} + \varphi_7 y_{11}; \\ I_5 - I_4 - I_6 = \varphi_2 y_{15} + \varphi_4 y_{14} - \varphi_5(y_{15} - y_{13} - y_{14}) + \varphi_6 y_{13}; \\ I_4 + I_8 = \varphi_4 y_{12} + \varphi_5 y_{13} - \varphi_6(y_{13} + y_{12} + y_{10} + y_9) + \varphi_7 y_{13} + \varphi_8 y_9; \\ 0 = \varphi_1 y_{18} + \varphi_4 y_{11} + \varphi_6 y_{13} - \varphi_7(y_{10} + y_{11} + y_2 + y_{18}) + U_{out} y_2 \\ I_2 + I_3 = \varphi_6 y_9 - \varphi_8(y_9 + y_4) + \varphi_9 y_4; \\ -(I_2 + I_1) = \varphi_8 y_4 - \varphi_9(y_4 + y_7 + y_5) + \varphi_{11} y_5 + \varphi_{10} y_7; \\ 0 = \varphi_9 y_7 + \varphi_{11} y_6 - \varphi_{10}(y_8 + y_7 + y_6); \\ I_1 - I_3 - U_{out} y_3 = \varphi_9 y_5 - \varphi_{11}(y_6 + y_5 + y_3) + \varphi_{10} y_6; \\ U_{out}(y_3 + y_2 + y_1) = \varphi_7 y_2 + \varphi_{11} y_3, \end{cases} \quad (1)$$

The conductivity of the circuit branches are determined by the equations:

$y_1 = 1/(Z_{24} + Z_7)$; $y_2 = 1/Z_{13}$; $y_3 = 1/Z_6$; $y_4 = 1/Z_3$; $y_5 = 1/Z_5$; $y_6 = 1/Z_4$; $y_7 = 1/Z_2$;
$y_8 = 1/(Z_{25} + Z_1)$; $y_9 = 1/(Z_8 + Z_9)$; $y_{10} = 1/Z_{12}$; $y_{11} = 1/Z_{11}$; $y_{12} = 1/Z_{10}$;
$y_{13} = (Z_{16} + Z_{14})/(Z_{16}Z_{14})$; $y_{14} = 1/Z_{15}$; $y_{15} = 1/Z_{17}$; $Y_{16} = 1/Z_{18}$; $y_{17} = 1/Z_{20}$;
$y_{18} = 1/Z_{22}$; $y_{19} = 1/Z_{21}$; $y_{20} = 1/Z_{19}$; $y_{21} = 1/Z_{23}$.

The active and reactive component of the impedance have been calculated in the software package MATLAB 8.1 using the system of equations (1). Calculated and experimental dependencies on gas concentration are shown in Fig. 4.

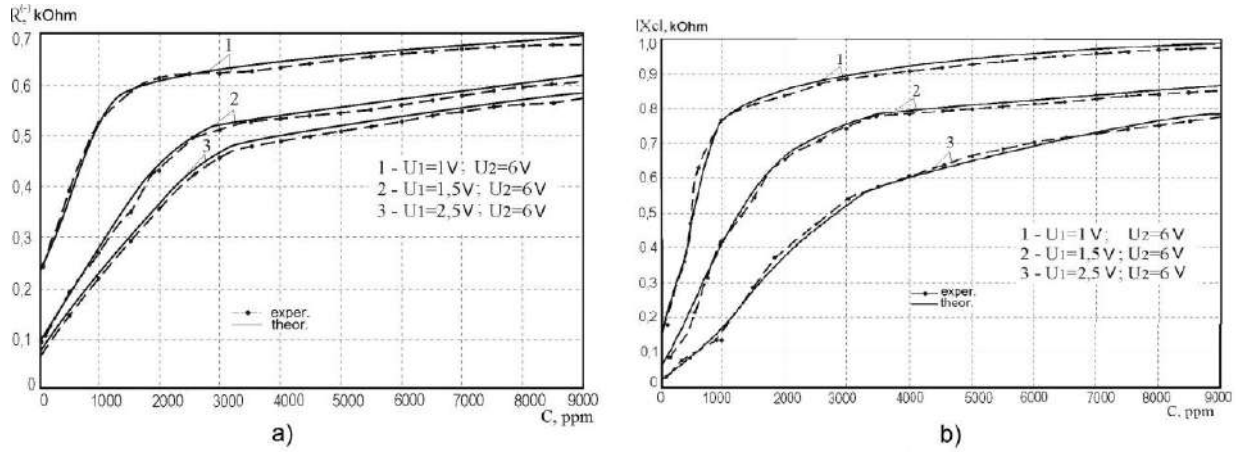


Fig. 4. Theoretical and experimental dependencies of active (a) and reactive (b) component of the impedance on gas concentration

Graphs in Fig. 4 show that active and reactive impedance components increase owing to the increased concentration of gas. Calculated and experimental dependencies of an active and reactive component of the impedance on the supply voltage U_1 are shown in Fig. 5.

The experimental dependencies of oscillation frequency of transducer of gas concentration on supply voltage U_1 and control voltage U_2 are presented in Fig. 6.

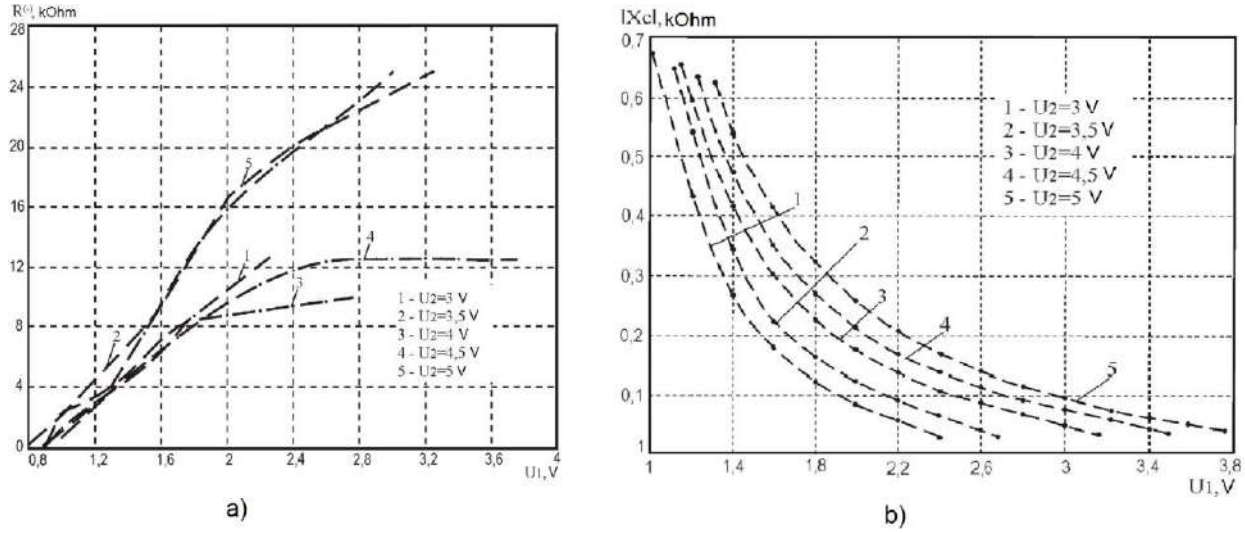


Fig. 5. Experimental dependencies of active (a) and reactive (b) component of the impedance on the supply voltage of transducer

Fig. 6 shows that an optimal mode of the transducer operation is the mode in which the oscillation frequency is linearly dependent on the supply voltage. Such mode matches the operation of transducer at the voltage control 4,5 – 5 V.

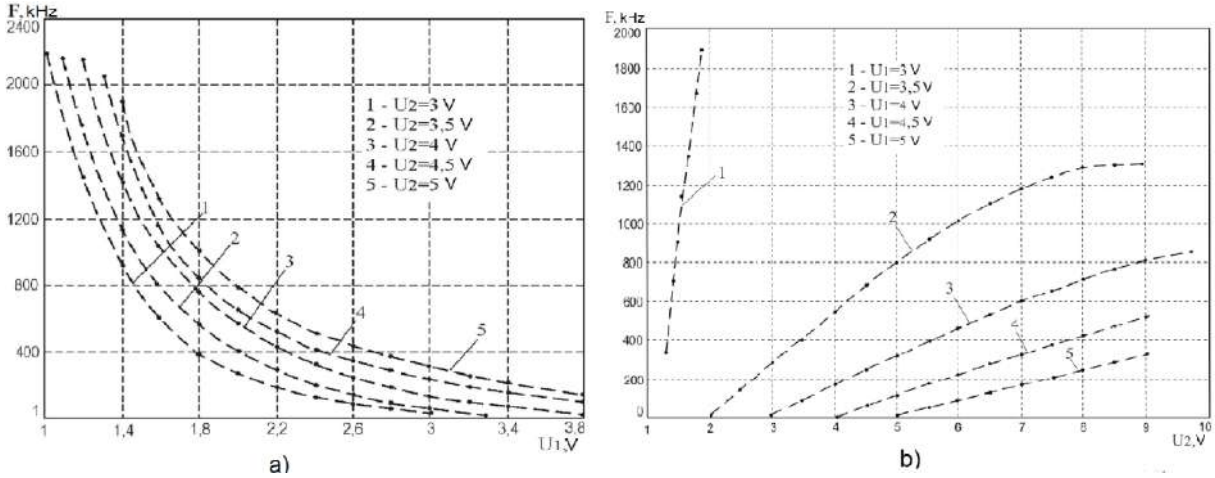


Fig. 6. Experimental dependencies of oscillation frequency on the supply (a) and control (b) voltage of transducer of gas concentration

One can show in Fig. 6 that the oscillator has a stable oscillation within the range from 5 V to 3 V and oscillation mode of the transducer of gas concentration should be selected within this range. The experimental and theoretical dependencies of oscillation frequencies of the transducer on the concentration of propane (C_3H_8) are presented in Fig. 7.

The dependence of the oscillation frequency of the gas concentration (transfer function) is determined by means of the circuit reverse current in accordance with the equivalent circuit (Fig. 3) based on Lyapunov stability theory [13]. The transfer function of radio measuring transducer is described by formula (2)

$$F = \frac{1}{2}\frac{\sqrt{2}\sqrt{L_1C_4(-L_1C_4 + R_1^2(C)C_3^2 + R_1^2(C)C_3C_{42} + A)}}{L_1C_3C_4R_1(C)}, \qquad (2)$$

where $A=\sqrt{L_1^2C_4^2+2L_1C_3^2C_4R_1^2(C)-B+R_1^4(C)C_3^2+D+R_1^4(C)C_3^2C_4^2}$; $B=2L_1C_4^2C_3R_1^2(C)$; $D=2C_3^3C_4R_1^4(C)$; C – concentration of gas (ppm).

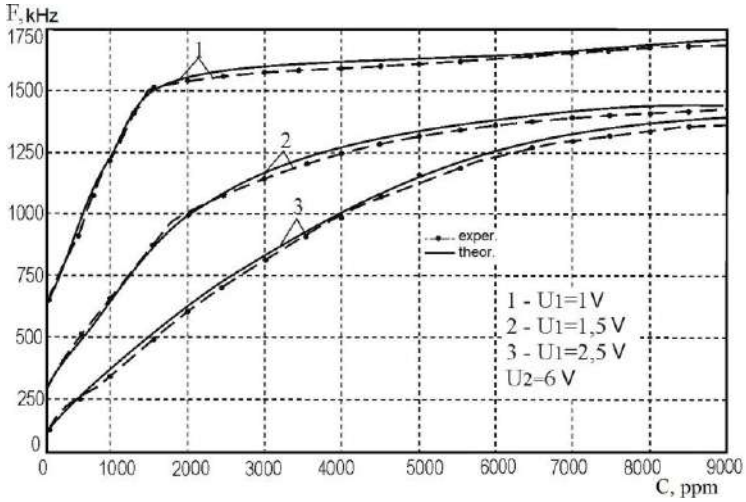


Fig. 7. Theoretical and experimental dependencies of oscillation frequency of transducer on propane (C_3H_8) concentration change

At increasing of gas concentration, the oscillation frequency raises and correlation of the oscillation frequency change and change of gas concentration is the most in the range within from 1ppm to 2000 ppm. The theoretical values agree with experimental data to within better than ± 5%.

The sensitivity of oscillation of the measuring transducer of gas concentration with MEMS resistive element MiCS 6814, sensitive to change of combustible gases concentration has been calculated having used the equation (2):

$$S_C^F=\frac{1}{4}\sqrt{2}\left(2R_1(C)C_3^2\left(\frac{\partial R_1(C)}{\partial C}\right)+2R_1(C)C_3C_4\left(\frac{\partial R_1(C)}{\partial C}\right)+\left(\frac{1}{2}\left(4L_1R_1(C)C_3^2C_4\left(\frac{\partial R_1(C)}{\partial C}\right)-\right.\right.\right.$$
$$-4L_1R_1\,(C)C_4^2C_3\left(\frac{\partial R_1(C)}{\partial C}\right)+4R_1^3(C)C_3^4\left(\frac{\partial R_1(C)}{\partial C}\right)+8R_1^3(C)C_3^3C_4\left(\frac{\partial R_1(C)}{\partial C}\right)+4R_1^3(C)C_3^2C_4^2\times$$
$$\left.\left.\left.\times\left(\frac{\partial R_1\,(C)}{\partial C}\right)\right)\Big/\sqrt{D_1}\right)\Big/\left(\sqrt{-L_1C_4(D_2+\sqrt{D_1})}\right)-\frac{1}{2}\sqrt{2}\sqrt{L_1C_4(D_2+\sqrt{D_1})}\times\right. \quad , (3)$$
$$\left.\times\left(\frac{\partial R_1(C)}{\partial C}\right)\Big/\left(L_1C_4C_3R_1^2(C)\right)\right),$$

where

$$D_1=L_1^2C_4^2+2L_1C_4C_3^2R_1^2(C)-2L_1C_4^2C_3R_1^2(C)+R_1^4(C)C_3^4+2R_1^4(C)C_3^3C_4+R_1^4(C)C_3^2C_4^2;$$
$$D_2=-L_1C_4+R_1^2(C)C_3^2+R_1^2(C)C_4C_3.$$

Figure 8 below includes the dependence of the sensitivity of the frequency transducer of gas concentration.

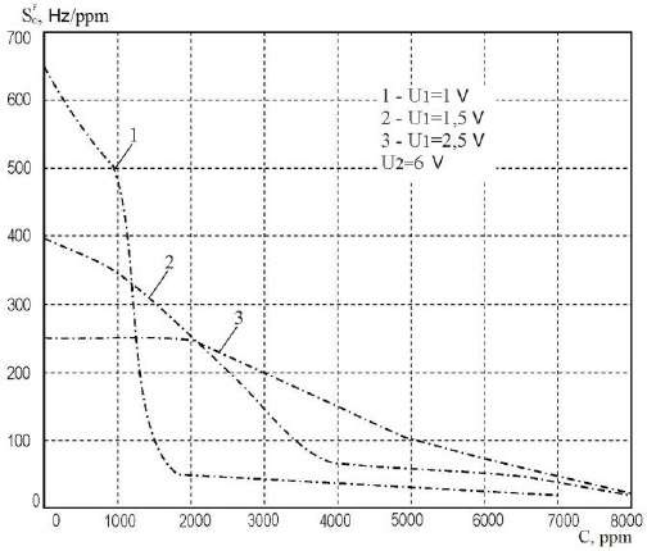


Fig. 8. The sensitivity of the transducer of gas concentration

The graphs in Fig. 8 illustrate that the transducer of gas concentration with MEMS resistive element MiCS 6814 has maximum sensitivity for supply voltage 1 V and control voltage 6 V. The sensitivity is significantly reduced by increasing the concentration of propane. It equals from 175 Hz/ppm to 48 Hz/ppm in the range 1500 ppm to 9000 ppm.

In order to test the design model for adequacy we can use the formula [14]

$$\delta_m = \frac{x_m - x_e}{x_e} \cdot 100\,\%, \tag{4}$$

where x_m – current value of the model; x_e – current experimental value of the parameter.

Fig. 9 shows the dependence of deviations of theoretical model on experimental values of gas concentration. As it is visible (Fig. 9), the divergence of experimental and theoretical data is ±5 %. The dependencies of oscillator frequency of transducer of gas concentration on temperature, are figured in fig.10. One can see that the oscillator frequency raises with increasing temperature. The optimal control voltage equals 3 V. At this voltage there is the slightest change of the oscillation frequency within the range from 20 °C to 80 °C.

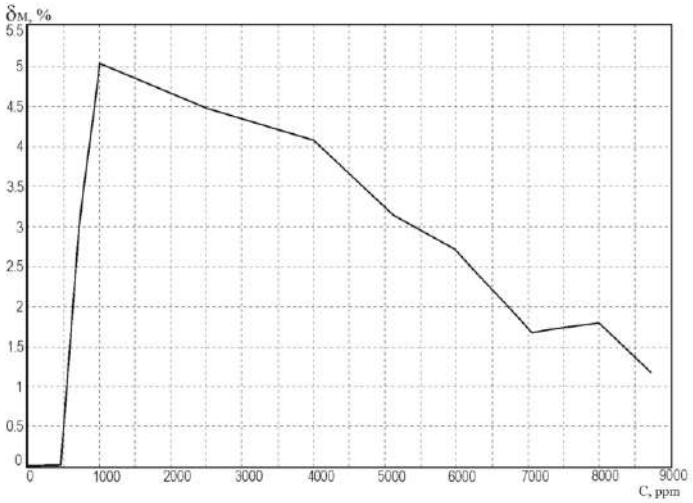


Fig. 9. Dependency of deviations of theoretical model
on experimental values of gas concentration

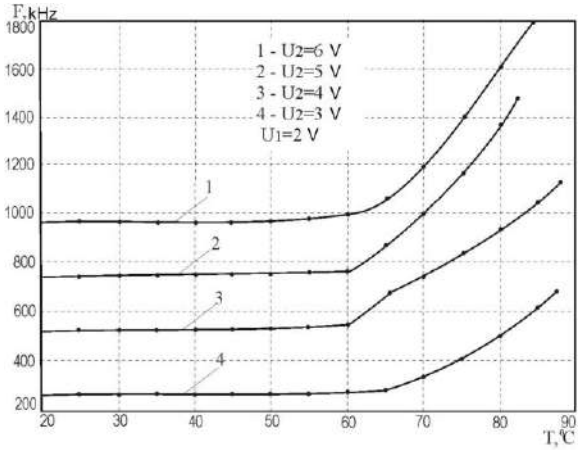


Fig. 10. Dependencies of oscillation frequency
of the transducer of gas concentration on temperature

CONCLUTIONS

The circuit of frequency transducer of gas concentration based on self-sustained oscillator was proposed. Results of the research of the frequency transducer of gas concentration with MEMS resistive element MiCS 6814, sensitive to the concentration change of combustible gases are reported. The dependencies of active and reactive components of the impedance of the frequency transducer of gas concentration on supply, control voltage and on gas concentration were calculated. Analytic expressions for transfer function and sensitivity equation were obtained.

The sensitivity of transducer of gas concentration changes from 645 Hz/ppm to 175 Hz/ppm in the range from 1 ppm to 1500 ppm. However, it substantially decreases with increasing propane concentration from 1500 ppm to 9000 ppm and changes from 175 Hz/ppm to 48 Hz/ppm within the range.

REFERENCES: 1. *Microelectronic* sensors of physical quantities. Edited Z.Yu..Hotra. In 3 volumes. – Lvov : League-Press, 2003. Vol.2. 2. *P.V. Novitsky, V.G. Knoring, V.S. Gutnikov*. Digital devices with frequency sensors. -Leningrad: Energy, 1970. 3. *Kwang-Jow Gan, Dong-Shong Liang, Chung-Chih Hsiao, Cher-Shiung Tsai and Yaw-Hwang Chen.* Investigation of MOS-NDR Voltage Controlled Ring Oscillator Fabricated by CMOS Process. 2005 // IEEE Conference on Electron Devices and Solid-State Circuits, 2005. pp. 825-827. DOI: 10.1109/EDSSC.2005.1635405. 4. *Kwang-Jow Gan, Kuan-Yu Chun, Wen-Kuan Yeh*. Design of Dynamic Frequency Divider using Negative Differential Resistance Circuit // International Journal on Recent and Innovation Trends in Computing and Communication. 2015. Volume: 3 Issue: 8. pp.5224-5228. 5. *J. Núñez, M. J. Avedillo and J. M. Quintana*. Bifurcation diagrams in MOS-NDR frequency divider circuits. 2012 // 19th IEEE International Conference on Electronics, Circuits, and Systems (ICECS 2012), Seville, 2012. pp. 480-483. DOI: 10.1109/ICECS.2012. 6463558. 6. D. *S. Liang, K. J. Gan and K. Y. Chun*. Frequency divider design using the Λ-type negative-differential-resistance circuit. 2010 53rd IEEE International Midwest Symposium on Circuits and Systems, Seattle, WA, 2010. pp. 969-972. DOI: 10.1109/MWSCAS.2010.5548795. 7. *Osadchuk A.V., Osadchuk V.S.* "Radiomeasuring Microelectronic Transducers of Physical Quantities". 2015 Proceedings of the International Siberian Conference on Control and Communications (SIBCON). 21-23 May 2015. Omsk. 978-1-4799-7103-9/15. DOI: 10.1109/SIBCON. 2015.7147167. 8. *V.S. Osadchuk, O.V. Osadchuk.* Reactive properties of transistors and transistor circuits. – Vinnitsa : UNIVERSUM-Vinnitsa, 1999. 9. *I.M. Vikulin and V.I. Stafeev*. Physics of semiconductor devices. Moscow: Radio and Communication, 1990. 10. *V.S. Osadchuk, O.V. Osadchuk, M.O. Prokopov.* Sensors of gas. Vinnitsa: UNIVERSUM. – Vinnitsa, 2008. 11. *Andrzej Smolarz; O. V. Osadchuk; D. P. Dudnyk; R. V. Krynochkin; W. Wojcik; A. Iskakova.* Mathematical model of radiation interaction with gas // Proc. SPIE 8698, Optical Fibers and Their Applications 2012, 86980U (January 11, 2013); doi:10.1117/12.2019734. 12. *O. Osadchuk, V. Osadchuk and I. Osadchuk*. The generator of superhigh frequencies on the basis silicon germanium heterojunction bipolar transistors // 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). Lviv, 2016, pp. 336-338. doi: 10.1109/TCSET.2016.7452051. 13. *Kayatskas A.A.* Basics of electronics. Moskow : Executive. wk., 1988. 14. *G.Ya. Mirsky*. Electronic measurements. Moscow : Radio and Communication, 1986.

Винницкий национальный
технический университет

Поступила в редколлегию 09.10.2017

УДК 534.843.26

В.В. УСИК, канд. техн. наук, И.Г. МЯГКИЙ

ОСОБЕННОСТИ ПРОВЕДЕНИЯ АКУСТИЧЕСКОГО МОДЕЛИРОВАНИЯ КАК ЗАВЕРШАЮЩЕГО ЭТАПА АКУСТИЧЕСКОЙ ЭКСПЕРТИЗЫ ПОМЕЩЕНИЙ ЗРИТЕЛЬНЫХ ЗАЛОВ НА ПРИМЕРЕ ДРАМАТИЧЕСКОГО ТЕАТРА НА 500 МЕСТ

Введение

Создание оптимальных акустических условий в зрительном зале зависит не только от выбранной системы звукоусиления, но и от соблюдения архитектурно-строительных рекомендаций, полученных на основе расчетов, выполненных тремя теориями распространения звуковых волн в помещении.

Акустические свойства помещения во многом определяются следующими факторами: объемом и формой помещения; количеством и наличием публики; размерами, формой, конструкциями ограждающих поверхностей; применяемых материалов отделки поверхности помещения и распределение их на поверхностях помещения.

В той или иной степени акустические свойства связаны с объективными и субъективными критериями оценки акустики помещения, такими как: гулкость-жизненность; пространственность; различимость и ясность; разборчивость; громкость; теплота; отсутствие эха.

Кроме перечисленных факторов, согласно [1 – 3], на каждом зрительском месте необходимо сформировать оптимальную структуру реверберационного процесса, который условно разделяется на два участка;

– *ранний*, для которого еще несправедливо условие диффузности поля, и поэтому для его формирования важна последовательность прихода дискретных отражений, время их прихода, а также направление прихода. Для формирования этого участка используется геометрическая теория, позволяющая проектировать ограждающие конструкции требуемой формы;

– *завершающий*, для которого уже справедливо понятие диффузности поля, а значит, для оценки используется статистическая теория распространения звука в помещении. Для формирования этого участка важна не только форма ограждающих поверхностей, но и использование соответствующих материалов отделки помещения и их распределение по поверхностям.

Таким образом, задачу акустической экспертизы можно разделить на три этапа:

- *проверки* существующих архитектурно-строительных решений внутренних поверхностей помещения с целью выявления фокусирующих звуковые лучи поверхностей (снижающих диффузность поля), а также получение частотной зависимости времени реверберации и сравнения с оптимальным временем реверберации [4 – 10];

- *выработки рекомендаций* с целью повышения диффузности звукового поля и обеспечения оптимальной структуры реверберационного процесса (этап создания технического задания на разработку конструкций ограждающих поверхностей) [4 – 10];

- *акустического моделирования* помещения с рекомендуемыми отделочными материалами и рекомендуемыми в техническом задании ограждающими поверхностями.

Цель работы

1. Разработка рекомендаций по использованию отделочных материалов для всех поверхностей зрительного зала для обеспечения оптимально частотной зависимости времени реверберации;

2. Проверка предложенных на I, II этапах акустической экспертизы проектных решений по геометрии стеновых и потолочных панелей [9, 10];

3. Моделирование акустических параметров помещения драматического тетра в программном пакете Ease 4.4 с учетом рекомендуемых материалов и архитектурно-строительных решений профилей потока и стен в зрительном зале;

4. Оценка предложенной системы озвучивания;
5. Анализ объективных параметров звукового поля в помещении;
6. Анализ структур реверберационных процессов на контрольных зрительских местах.

Основная часть

Для исследования акустических свойств помещения была создана модель помещения драматического тетра в Ease 4.4 (рис.1 – 2), которая учитывает все особенности геометрии стеновых панелей, потолочных, а также в ней учтено наличие зрительских мест со свойственным звукопоглощением и одежда сцены [6 – 10].

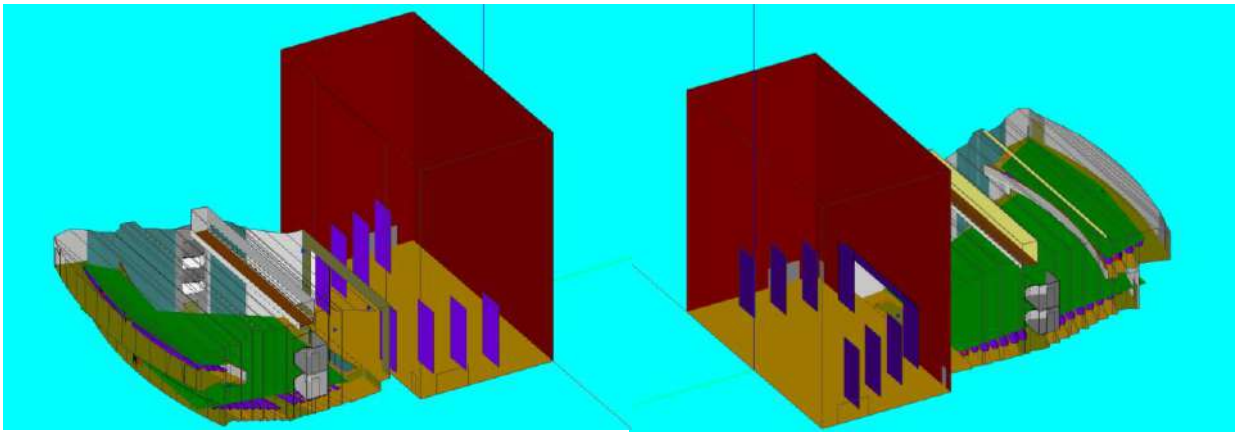


Рис. 1. Вид модели помещения в Ease 4.4

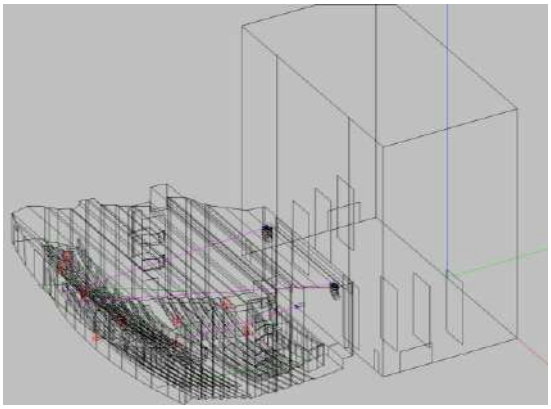


Рис. 2. Модель помещения в Ease 4.4

Проектные предложения по отделке помещения

1. Материалы отделки стен помещения сценической коробки (рис. 3) представлены в табл. 1

Таблица 1

Позиция	Название поверхности	Отделочный материал
1	Задняя стена сценической коробки	Звукопоглощающие панели Heradesign Superfine 25 мм, на относе 250 мм с заполнением минеральной ватой
2	Боковые стены сценической коробки	Звукопоглощающие панели Heradesign Superfine 25 мм, на относе 250 мм с заполнением минеральной ватой
3	Портальная стена сценической коробки	CLAY BRICK, кирпичная кладка
4	Часть портальной стены, примыкающая к зрительному залу (со стороны зала)	PLAST/LTHS, штукатурка гладкая по кирпичу или МДФ панели Décor Acoustic.

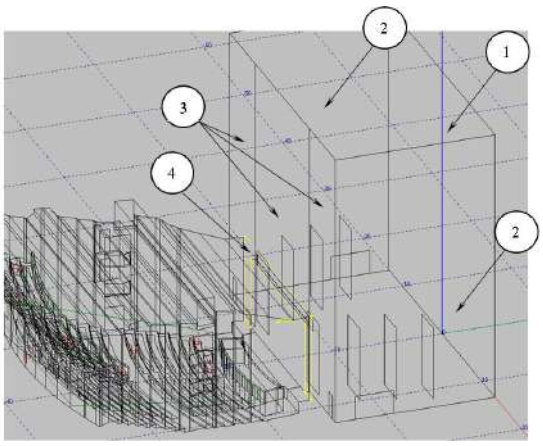


Рис. 3. Вид модели сценической коробки

2. Материалы отделки стен помещения зрительского зала (рис. 4, табл.2).

Таблица 2

Позиция	Отделочный материал
1	Листы гипсокартона 12,5 мм в два слоя (ГКЛ) или MDF панели Décor Acoustic
2	Перфорированные гипсокартонные звукопоглощающие плиты KNAUF_Perfpanel_B5-12/25Q

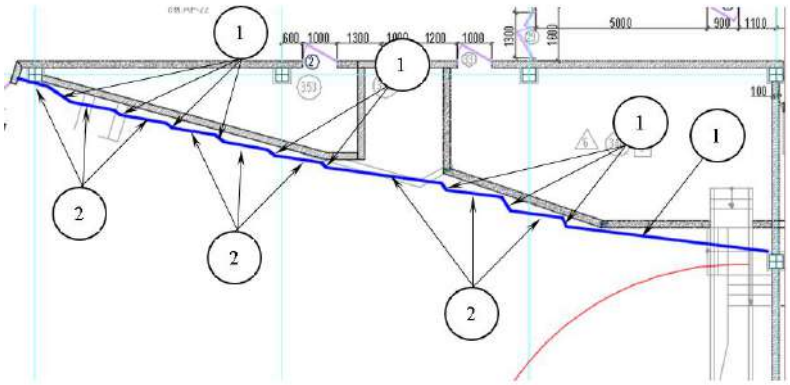


Рис. 4. Профиль стеновых панелей с обозначением отделочных материалов

3. Материалы отделки профиля потолка зрительного зала (рис. 5, табл.3).

Таблица 3

Позиция	Отделочный материал
1	Листы гипсокартона 12,5 мм в два слоя (ГКЛ)
2	Перфорированные гипсокартонные звукопоглощающие плиты KNAUF_Perfpanel_B5-12/25Q

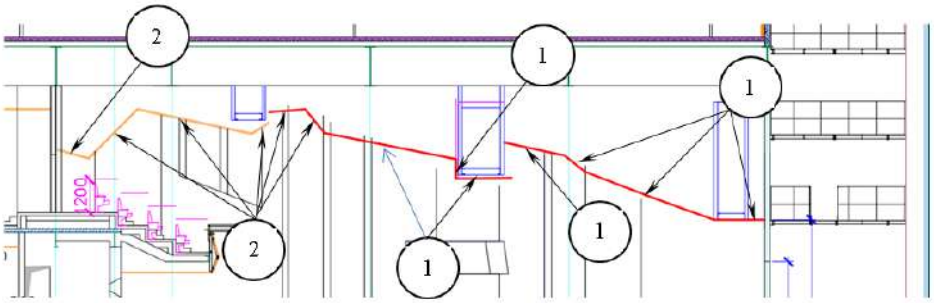


Рис. 5. Профиль потолочных звукоотражающих конструкций

4. Материалы отдела помещения выносного софита представлены на рис. 6 и в табл. 4.

Таблица 4

Позиция	Название поверхности	Отделочный материал
1	Задняя стена и потолок помещения выносного софита	Перфорированные гипсокартонные звукопоглощающие плиты KNAUF_Perfpanel_B5-12/25Q
2	Передняя стена помещения выносного софита	Листы гипсокартона 12,5 мм в два слоя (ГКЛ)
3	Пол помещения выносного софита	Конструктивный пол, покрытый линолеумом
4	Боковые стены помещения выносного софита	Листы гипсокартона 12,5 мм в два слоя (ГКЛ)

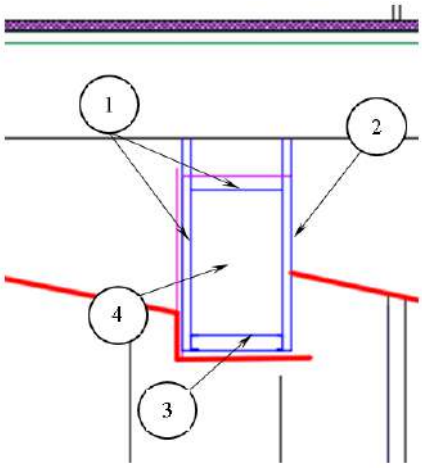


Рис. 6. Помещение выносного софита с обозначением отделочных материалов

5. Материалы отделки пола. Для обработки планшета сцены используется палубный брус 50 х 80 (высота) мм. Для настила пола зрительного зала – партера и балкона – используется паркет. Использование коврового покрытия нецелесообразно, так как это может привести к дополнительному нежелательному звукопоглощению на средних и высоких частотах.

6. Зрительские места. Свободные зрительские места должны обеспечивать определенное звукопоглощение для того, чтобы снизить зависимость времени реверберации от присутствия зрителей (особенно это важно во время проведения репетиций). Тогда, верхняя сторона поверхности сиденья и внутренняя сторона спинки сиденья должны быть обиты обивочным материалом (толщиной минимум 10 см) из пористого поролона с покрытием из ткани. Наружные поверхности сидений (которые не соприкасаются с сидящим человеком, т.е. задняя поверхность спинки сиденья и нижняя поверхность самого сиденья) должны сохранять отражающие способности во избежание чрезмерного дополнительного звукопоглощения, когда место занято. Когда место занято, звукопоглощающую функцию, в основном, должен выполнять сам сидящий человек, а не сиденье.

Коэффициент звукопоглощения (допуск ± 0,1) незанятого зрительского места должен быть следующим (табл. 5).

Таблица 5

Частота, Гц	125	250	500	1000	2000	4000
Коэффициенты звукопоглощения	0,3	0,5	0,7	0,8	0,8	0,8

Правильная обивка из ткани (которая часто применяется в зрительных залах) также может обеспечить необходимое звукопоглощение в пустом зале.

7. Отделка ограждения балкона зрительного зала. Рекомендуется применить акустические MDF панели Décor Acoustic со стороны зрительного зала. Со стороны зрителей внутреннюю поверхность ограждения балкона оштукатурить и окрасить в желаемый цвет по проекту архитекторов.

8. Материалы отделки оркестровой ямы. Обработка поверхностей оркестровой ямы представлена на рис. 7 и в табл. 6.

Таблица 6

Позиция	Название поверхности	Отделочный материал
1	Передняя стенка	Звукопоглощающий материал SUPER-G
2	Задняя стенка, боковые и внешние поверхности оркестровой ямы	Деревянные панели MDF Décor Acoustic
3	Пол	Паркет

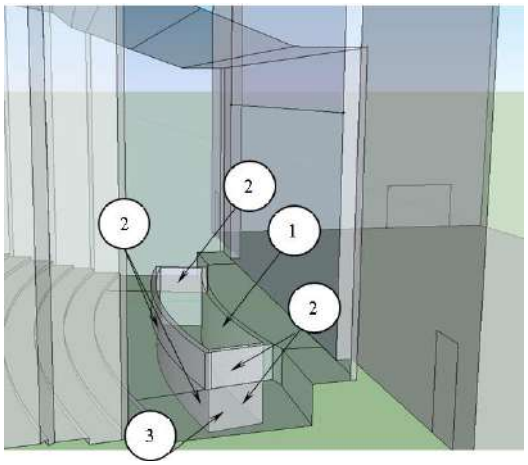
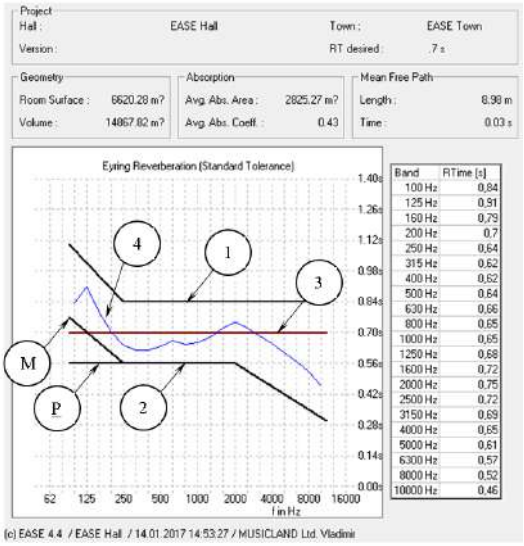


Рис. 7. Оркестровая яма с обозначением отделочных материалов

9. Двери. Двери филенчатые массивные – материал дерево, МДФ. Толщина полотна 35 – 40 мм. Во входных-выходных тамбурах для потока публики необходимо установить распашные двери в створе с внутренними стенами зала.

Результаты моделирования акустики помещения зрительного зала. График частотной зависимости времени реверберации для помещения драматического театра, полученный в EASE 4.4, представлен на рис.8.



1 – граница максимальных значений;
2 – граница минимальных значений; P – для речи;
M – для музыки;
3 – оптимальная величина RT60
(идеальная теоретическая) ;
4 – расчетная величина RT60 в диапазоне частот

Рис. 8.График частотной зависимости времени реверберации
для помещения драматического театра (RT 60)

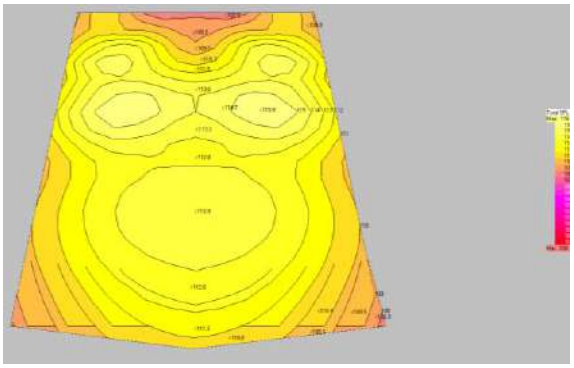


Рис. 9. Суммарный уровень звукового давления на зрительских местах

Оценка предложенной системы озвучивания. На рис. 9 представлен суммарный уровень звукового давления (Total SPL) на зрительских местах, развиваемый акустическими системами.

Анализ полученных результатов показывает, что предложенная система звукоусиления зала обеспечивает на всей площади зрительских мест звуковое давление в диапазоне от 107 до 115 дБ. Наименьшие значения развиваемого звукового давления находятся в области прохода между первым рядом и оркестровой ямой и в углах помещения около задней стенки, где также находятся проходы.

Анализ уровня прямого звука (Direct SPL) на зрительских местах также показывает достаточной уровень развиваемого звукового давления на всех площади прослушивания (рис. 10).

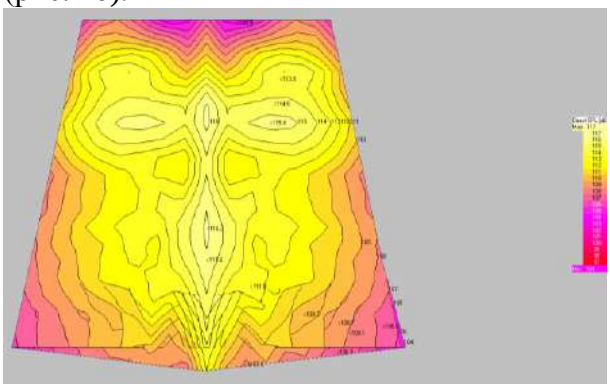


Рис. 10. Уровень прямого звука (Direct SPL) на зрительских местах

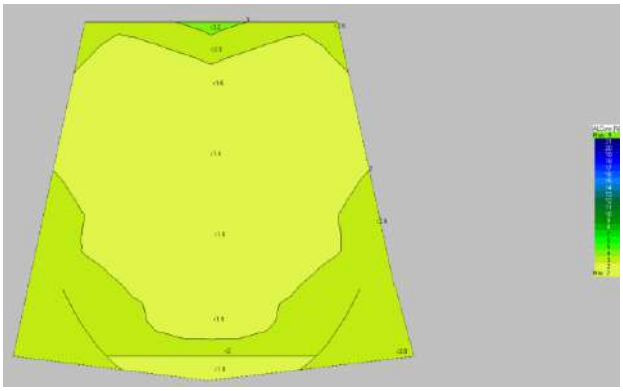


Рис. 11. Результаты расчета процента артикуляционных потерь Al_{cons}

Различимость и ясность. Для оценки разборчивости используется такие показатели, как: %ALcons (percentage Articulation Loss of Consonants) – процент артикуляционных потерь согласных; STI (speech transmission index) – индекс передачи речи; Al_{cons} – это альтернативный показатель объективной оценки речевой ясности в помещении или для систем звукоусиления.

На рис. 11 представлен результат расчета процента артикуляционных потерь для проектируемого помещения зрительного зала драматического театра.

Анализ результатов позволяет сделать вывод о практически *идеальной* полученной речевой ясности на всех зрительских местах – $\mathbf{Al_{cons}}$<3%.

На рис. 12 приведены результаты расчета STI для всей площади зрительских мест: полученные значения коэффициента лежат в пределах от 0,74 до 0,93, что соответствует критерию от *хорошо* до *отлично*.

Ясность. Оценка качества акустики помещений представлена объективными качественными критериями: показателем прямого звука C7; показателем речевой ясности C50; показателем музыкальной ясности C80.

На рис. 13 представлены результаты расчета уровня прямого звука на всей площади зоны прослушивания.

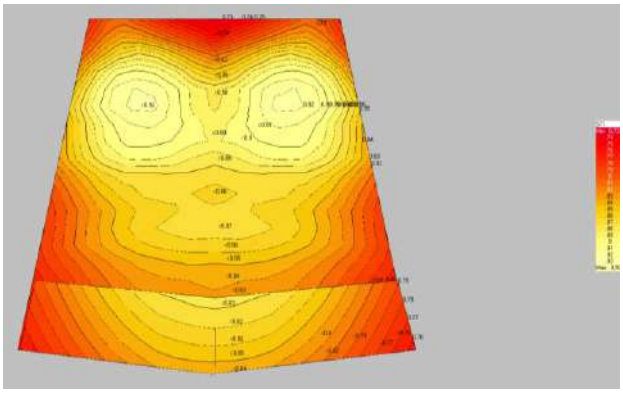


Рис. 12. Результаты расчета индекс передачи речи (STI)

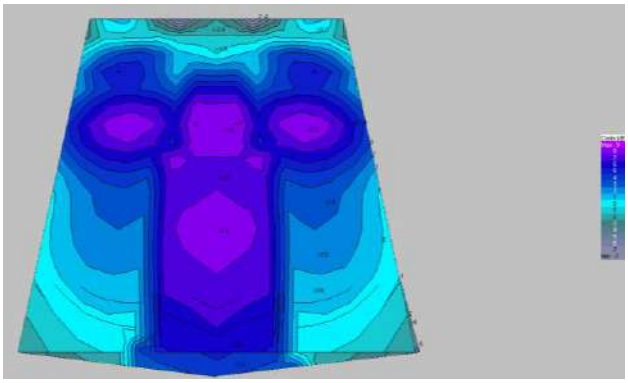


Рис. 13. Результаты расчета показателей прямого звука C_7

Анализ результатов позволяет сделать следующий вывод: уровень прямого сигнала, приходящий на всю площадь зрительских мест имеет достаточный уровень (C_7>-2 дБ), что позволит слушателям ощущать себя в «непосредственной» близости к источнику. Значение показателя прямого сигнала C_7<-2 дБ наблюдается только в местах зрительского зала, в ко-

торых находятся проходы перед оркестровой ямой и в боковых проходах, расположенных ближе к задней стенке зала, что не способствует ухудшению общего впечатления об акустике зала.

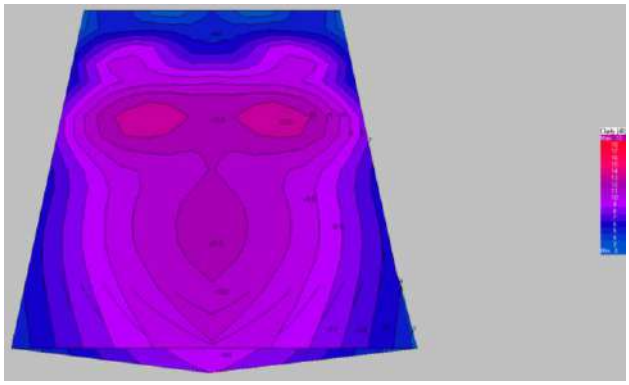


Рис. 14. Результаты расчета показателем речевой ясности C_{50}

На рис. 14 представлены результаты расчета показателя речевой ясности.

Анализ результатов позволяет сделать следующий вывод: на всей площади зрительских мест показатель речевой ясности превышает значение -2 дБ, что способствует достаточно высокой ясности слога и разборчивости речевого сигнала. Данный показатель очень важен для залов драматических театров, где основным звуковым материалом является речевой сигнал (речь актера).

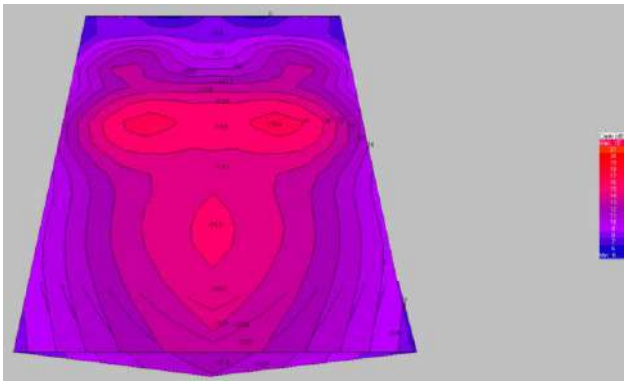


Рис. 15. Результаты расчета показателем музыкальной ясности C_{80}

На рис. 15 представлены результаты расчета показателя музыкальной ясности.

Анализ показателя музыкальной ясности на всей площади зрительских мест говорит о преобладании энергии ранних отражений по сравнению с энергией поздних отражений. Этот факт является приемлемым вариантом распределения энергии ранних и поздних реверберирующих звуков, так как для обеспечения достаточно высоких показателей качества передачи речевого сигнала наличие большей энергии реверберирующих звуков приведет к снижению разборчивости речевого материала.

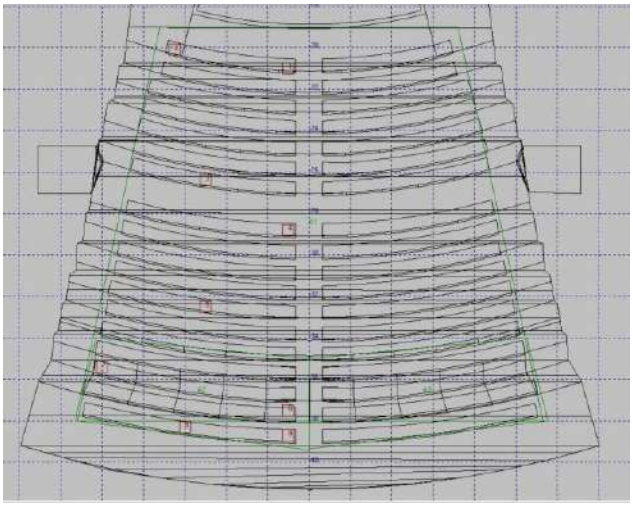


Рис. 16. Местоположение контрольных точек

Анализ структур реверберационных процессов в контрольных точках

Для оценки структуры реверберационного процесса на зрительских местах и оценки времени реверберации на каждом зрительском месте были выбраны характерные расчетные контрольные точки. На рис. 16 представлены местоположения 9 контрольных точек, расположенных в зрительском зале.

На рис. 17 – 20 представлены структуры реверберационных процессов на каждом месте прослушивания (контрольной точке).

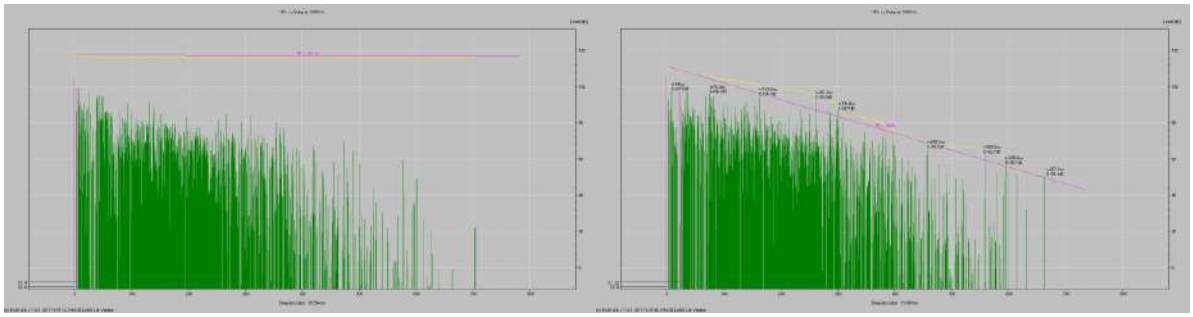


Рис. 17. Структуры реверберационного процесса в 1, 2 контрольных точках

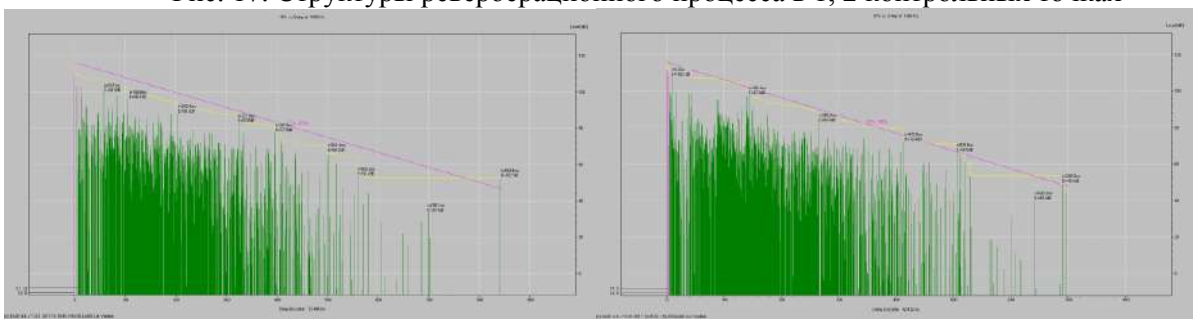


Рис. 18. Структуры реверберационного процесса в 3, 4 контрольных точках

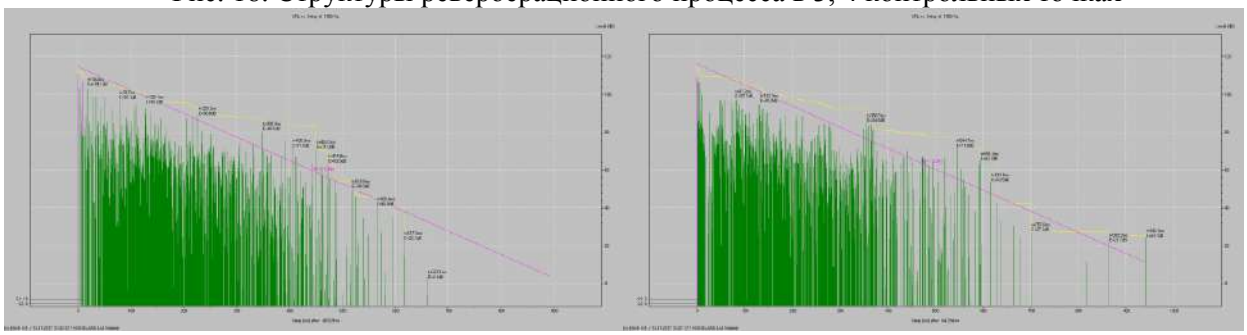


Рис. 19. Структуры реверберационного процесса в 5, 6 контрольных точках

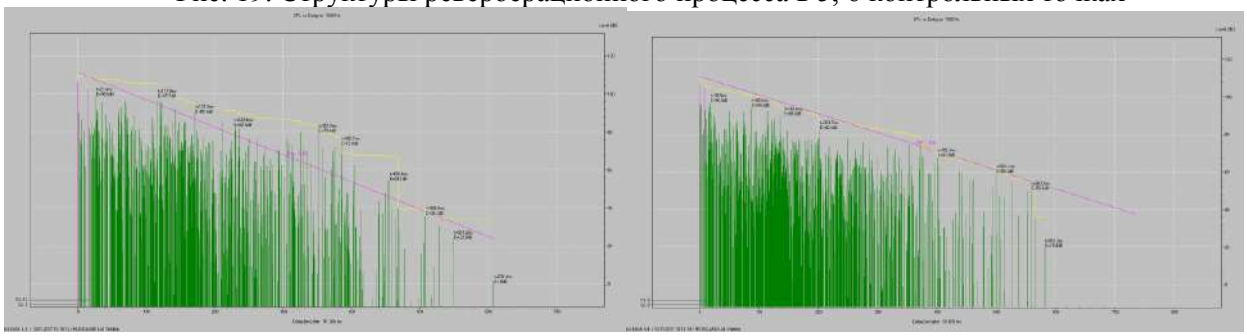


Рис. 19. Структуры реверберационного процесса в 7, 8 контрольных точках

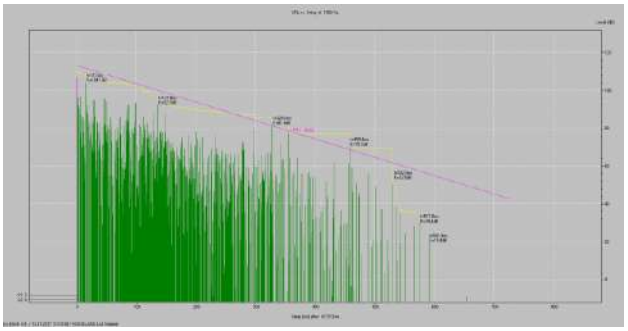


Рис. 20. Структура реверберационного процесса в 9 контрольной точке

Анализ структур реверберационных процессов на контрольных зрительских местах:

- на всех зрительских местах наблюдается достаточно высокая плотность отражений, что происходит при хорошей диффузности поля;
- уровни отраженных сигналов имеют плавную тенденцию к снижению амплитуды пришедших отражений, что обеспечивает равномерный, а не скачкообразный спад плотности звуковой энергии;
- время реверберации в контрольных точках попадает в предельные отклонения от

оптимального времени реверберации для зала, что позволит обеспечить практически одинаковое ощущение времени реверберации на каждом зрительском месте;

- на всех контрольных точках отсутствуют отражения, которые могли бы создавать ощущения эха.

Анализ направлений прихода ранних отражений позволяет сделать вывод об обеспечении ранних боковых отражений, что способствует формированию ощущения пространственности звучания, а также ранних отражений, пришедших с других направлений, что обеспечивает ощущение обёртываемости.

Выводы

Описанные результаты моделирования акустических свойств зрительного зала позволили проверить решения, принятые на первых двух этапах акустической экспертизы [9].

Моделирование помещения в программном пакете Ease 4.4 позволило авторам проанализировать систему озвучивания, объективные критерии акустического качества помещения, проанализировать структуры реверберационных процессов в контрольных точках, что имеет важное значение для зала драматического театра, где основным музыкальным материалом является речевой сигнал.

При проведении всех этапов акустической экспертизы не были учтены результаты, полученные с помощью волновой теории распространения звука в помещении, так как первые дискретные резонансы зала (с достаточно большими геометрическими размерами) будут лежать в низкочастотной области и в плохо слышимом диапазоне, что не приведет к искажению тембра звукового материала.

Список литературы: 1. *Макриненко, Л. И.* Акустика помещений общественных зданий. – М. : Стройиздат, 1986. – 173 с. 2. *Справочник* по акустике ; под ред. М. А. Сапожкова. – М. : Связь, 1979. – 312 с. 3. *Ковригин, С. Д., Крышов, С. И.* Архитектурно-строительная акустика. – М. : Высш. шк., 1986. – 256 с. 4. *Рейхардт, В.* Акустика общественных зданий ; пер. с нем. – М. : Стройиздат, 1984. – 198 с. 5. *Щиржецкий, Х. А., Борисов, Л. А.* Акустика зальных помещений // Сцена. – 2002. – №2 (21). 6. *Усик, В.В., Мягкий, И.Г.* Автоматизированный акустический расчет помещений зрительных залов с использованием статистической теории // Східноєвропейський журнал передових технологій. – Харків, 2010. – №3/11. – С.22-26. 7. *Усик, В.В., Мягкий, И.Г.* Применение геометрической теории для построения профиля зукоотражающей поверхности // Зб. наук. праць Харківського університету Повітряних Сил. – Харків, 2011. – Вип.1 (27). – с. 166-169. 8. *Усик, В.В., Мягкий, И.Г.* Комплексная оценка акустических свойств зала на примере проектирования "Центра воспитательной работы со студентами ХНАГХ" // Технология приборостроения. – Харьков, 2010. – №1. – С. 34-38. 9. *Порошин, С.М., Усик, В.В.* Методика проведения акустической экспертизы и архитектурно-строительных решений для зрительных залов на примере драматического театра на 500 мест // Зб. наук. праць. VI Міжнародний Радіоелектронний Форум “Прикладна радіоелектроніка. Стан та перспективи розвитку“ (МРФ – 2017). – Харьков, 2017. – С. 125-130.

Национальный технический университет
«Харьковский политехнический институт»,
ООО «Musicland»

Поступила в редколлегию 11.11.2017

РЕФЕРАТЫ РЕФЕРАТИ ABSTRACTS

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

УДК 004.056.55

Оптимизация алгоритма направленного шифрования NTRU Prime / *Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, О.С. Акользина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 5 – 10.

Показаны результаты оптимизации алгоритмов для постквантового механизма направленного шифрования NTRU Prime: приведение по модулю, вычисление ослепляющего полинома, алгоритма зашифрования и расшифрования. Приведен сравнительный анализ различных способов умножения полиномов.

Табл. 3. Библиогр.: 8 назв.

УДК 004.056.55

Оптимізація алгоритму направленого шифрування NTRU Prime / *О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, О.С. Акользіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 5 – 10.

Наведено результати оптимізації алгоритмів для постквантового механізму направленого шифрування NTRU Prime: зведення за модулем, обчислення засліплюючого поліному, алгоритмів зашифрування та розшифрування. Наведено порівняльний аналіз різних способів множення поліномів.

Табл. 3. Бібліогр.: 8 назв.

UDC 004.056.55

Optimization of NTRU Prime asymmetric encryption algorithm / *O.G. Kachko, Yu. I. Gorbenko, M.V. Esina, O.S. Akolzina* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 5 – 10.

The results of algorithms optimization for the post-quantum mechanism of asymmetric encryption NTRU Prime are given. Namely: module reduction, blinding polynomial calculation, encryption and decryption algorithms. A comparative analysis of different polynomials multiplications is also given

3 tab. Ref.: 8 items.

УДК 004.056.55

Анализ алгоритма направленного шифрования NTRU PRIME IIT UKRAINE с учетом известных атак / *И.Д. Горбенко, О.Г. Качко, М.В. Есина* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 11 – 23.

Рассмотрены современные криптографические преобразования типа «направленное шифрование» – NTRU-подобные криптосистемы. На основе криптопреобразований этого типа создана новая криптографическая система NTRU PRIME IIT UKRAINE. Кратко описана эта криптосистемы и проанализирована ее устойчивость к известным атакам, сделаны выводы и приведены рекомендации.

Ключевые слова: атака, кольцо, направленное шифрование, поле, фактор кольцо.

Библиогр.: 27 назв.

УДК 004.056.55

Аналіз алгоритму направленого шифрування NTRU PRIME IIT UKRAINE з урахуванням відомих атак / *І.Д. Горбенко, О.Г. Качко, М.В. Єсіна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 11 – 23.

Розглянуто сучасні криптографічні перетворення «направлене шифрування» – NTRU-подібні криптосистеми. На основі криптоперетворень цього типу створено нову криптографічну систему NTRU PRIME IIT UKRAINE. Наведено короткий опис цієї криптосистеми та проаналізовано її стійкість до відомих атак, зроблено висновки та наведено рекомендації.

Ключові слова: атака, кільце, направлене шифрування, поле, фактор кільце.

Бібліогр.: 27 назв.

UDC 004.056.55

Analysis of the end-to-end encryption algorithm NTRU PRIME IIT UKRAINE taking into account known attacks / *I.D. Gorbenko, O.G. Kachko, M.V. Yesina* // Radiotekhnika : All-Ukr. Sci. Interdep.

Mag. – 2017. – №191. – P. 11 – 23.

Modern cryptographic transformations of the end-to-end encryption type, namely – NTRU-like cryptosystems are considered. A new cryptographic system NTRU PRIME IIT UKRAINE was created based on existing cryptographic transformations of this type. A brief description of this cryptosystem is presented and an analysis of its resistance to known attacks is carried out, conclusions are made and recommendations are given.

Key words: attack, ring, end-to-end encryption, field, factor ring.

Ref.: 27 items.

УДК 004.056.55

Усовершенствованный механизм одноразовых ключей для постквантового периода на основе хеш-функций / *Ю.И. Горбенко, Е.В. Исирова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 24 – 39.

Обоснована необходимость разработки новых механизмов электронной подписи, которые будут актуальными и смогут применяться в постквантовый период. Приведены основные свойства существующих механизмов, их преимущества и недостатки. Предложен усовершенствованный механизм POTS. Изложена сущность, представлены исследования свойств по критериям сложность – криптографическая стойкость, определены преимущества и недостатки, а также условия и возможности его применения в различных приложениях постквантового периода.

Табл. 9. Библиогр.: 14 назв.

УДК 004.056.55

Удосконалений механізм одноразових ключів для постквантового періоду на основі геш-функцій / *Ю І. Горбенко, К.В. Ісірова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 00 – 24 – 39.

Обґрунтовано необхідність розробки нових механізмів електронного підпису, які будуть актуальними та можуть застосовуватись у постквантовий період. Наведено основні властивості існуючих механізмів, їх переваги та недоліки. Запропоновано удосконалений механізм POTS. Викладена сутність, дослідження властивостей за критеріями складність – криптографічна стійкість, визначено переваги та недоліки, а також умови і можливості його застосування в різних додатках постквантового періоду.

Табл. 9. Бібліогр.: 14 назв.

UDC 004.056.55

Improved Post-quantum Hash Based One-Time Key Mechanism / *Yu.I. Gorbenko, K.V. Isirova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 24 – 39.

The necessity of developing new electronic signature mechanisms, which will be relevant and can be applied in the post-quantum period, is grounded. The main properties of existing mechanisms, their advantages and disadvantages are given. An improved POTS mechanism is proposed. The essence is described, research of properties by criteria of complexity - cryptographic stability is presented, advantages and disadvantages and conditions and possibilities of its use in various applications of the post-quantum period are determined..

9 tab. Ref.: 14 items.

УДК 681.3.06

Оценка пропускной способности платформы Ethereum на основе математической модели смарт-контракта / *Н.Е. Иванов, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 40 – 46.

Предложена математическая модель для смарт-контрактов начального размещения токенов (ICO), широко применяемых на платформе Ethereum. Проведен анализ зависимости пропускной способности сети от таких параметров, как размер буфера заявок, среднее время обработки заявки. Получены оценки того, какие параметры имеют наибольшее влияние на пропускную способность Ethereum в рамках разработанной модели.

Ил. 4. Библиогр.: 13 назв.

УДК 681.3.06

Оцінка пропускної здатності платформи Ethereum на основі математичної моделі смарт-контракту / *М.Е. Іванов, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 40 – 46.

Запропоновано математичну модель для смарт-контрактів початкового розміщення токенів (ICO), що широко застосовуються на платформі Ethereum. Проведено аналіз залежності пропускної здатності від таких параметрів, як розмір буфера заявок, середній час обробки заявки. Отримано оцінки того, які параметри мають найбільший вплив на пропускну здатність Ethereum в рамках розробленої моделі.

Іл. 4. Бібліогр.: 13 назв.

UDC 681.3.06

Estimating the capacity of the Ethereum platform based on the mathematical model of the smart contract / M. *Ivanov, R. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 40 – 46.

A mathematical model for smart contracts for deployment of the initial coin offering (ICO), widely used on the Ethereum platform, is proposed. The analysis of dependence of the network capacity on such parameters as the transaction buffer size, the average transaction processing time, is performed. Evaluations are obtained of which parameters have the greatest impact on the capacity of Ethereum within the developed model.

4 fig. Ref.: 13 items.

УДК 621.3.06

Методы поиска дифференциальных характеристик цикловой функции симметричного блочного шифра «Кипарис» / *М.Ю. Родинко, Р.В. Олейников* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 47 – 51.

Предложены три метода поиска дифференциальных характеристик цикловой функции блочного шифра «Кипарис»: прямой метод поиска, метод поиска «в двух направлениях» и оптимизированный метод поиска дифференциальной характеристики с высокой вероятностью. Цель всех трех подходов – активизация наименьшего количества бит на входах сумматоров цикловой функции, что, в свою очередь, увеличивает вероятность заданного преобразования. Оптимизированный метод позволил найти дифференциальную характеристику цикловой функции блочного шифра «Кипарис» с вероятностью, равной ¼.

Табл. 4. Ил. 1. Библиогр: 9 назв.

УДК 621.3.06

Методи пошуку диференційних характеристик циклової функції симетричного блокового шифру «Кипарис» / *М.Ю. Родінко, Р.В. Олійников* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 47 – 51.

Запропоновано три методи пошуку диференційних характеристик циклової функції блокового шифру «Кипарис»: прямий метод пошуку, метод пошуку «у двох напрямках» та оптимізований метод пошуку диференціальної характеристики з високою ймовірністю. Мета всіх трьох підходів – активізація найменшої кількості біт на входах суматорів циклової функції, що, в свою чергу, збільшує ймовірність заданого перетворення. Оптимізований метод дозволив знайти диференційну характеристику на циклову функцію блокового шифру «Кипарис» з ймовірністю, яка дорівнює ¼.

Табл. 4. Іл. 1. Бібліогр: 9 назв.

UDC 621.3.06

Methods for finding differential characteristics of block cipher «Cypress» / *M.Yu. Rodinko, R.V. Oliynykov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 47 – 51.

Three methods for finding differential characteristics of the round function of the block cipher «Cypress» are proposed, namely: a direct search method, a two-way search method, and an optimized method for finding the differential characteristic with high probability. The purpose of all three approaches is to activate the smallest amount of bits at inputs of the modulo addition transformation of the round function, which, in turn, increases the likelihood of the transformation. The optimized method makes it possible to find the differential characteristic on the round function of the block cipher "Cypress" with a probability that equals ¼.

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

УДК 004.056.55

Сравнительные исследования алгоритмов потокового криптографического преобразования / *А.А. Кузнецов, Д.В. Иваненко, М.С. Луценко, В.А. Тимченко, О.М. Мелкозерова, М.О. Осадчук, Е.В. Острянская* // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 52 – 75.

Изложены основные результаты сравнительных исследований алгоритмов потокового крипто-

графического преобразования, в частности стандартизированных в ISO / IEC 18033-4, ISO / IEC 29192-3 и представленных в качестве победителей международных проектов eSTREAM и CRYPTREC. Сравнительные исследования проводились по двум направлениям: во-первых, исследовалась статистическая безопасность путем тестирования выходных последовательностей; во-вторых, оценивалось быстродействие генераторов в определенных режимах практического применения. Обоснованы наиболее перспективные направления дальнейших исследований по вопросам разработки и применения нового потокового шифра в Украине.

Табл. 10. Ил. 40. Библиогр: 24 назв.

УДК 004.056.55

Порівняльні дослідження алгоритмів потокового криптографічного перетворення / *О.О. Кузнецов, Д.В. Іваненко, М.С. Луценко, В.А. Тимченко, О.М. Мелкозерова, М.О. Осадчук, Є.В. Острянська* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 52 – 75.

Викладено основні результати порівняльних досліджень алгоритмів потокового криптографічного перетворення, зокрема стандартизованих у ISO/IEC 18033-4, ISO/IEC 29192-3 та представлених у якості переможців міжнародних проектів eSTREAM та CRYPTREC. Порівняльні дослідження проводилися за двома напрямками: по-перше, досліджувалася статистична безпека шляхом тестування вихідних послідовностей; по-друге, досліджувалася швидкодія генераторів у певних режимах застосування. Обґрунтовано найбільш перспективні напрямки подальших досліджень з питань розробки та застосування нового потокового шифру в Україні.

Табл. 10. Іл. 40. Бібліогр: 24 назви.

UDC 004.056.55

Comparative studies of flow cryptographic transformation algorithms / *O.O. Kuznetsov, D.V. Ivanenko, M.S. Lutsenko, V.A. Timchenko, OM Melkozerova, M.O. Osadchuk, Є.V. Ostryanska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 52 – 75.

The main results of comparative studies of flow cryptographic transformation algorithms are described, in particular those ones standardized in ISO / IEC 18033-4, ISO / IEC 29192-3 and presented as winners of international projects eSTREAM and CRYPTREC. Comparative studies were carried out in two directions: first, statistical safety was investigated by testing the output sequences; secondly, the speed of the generators in certain modes of practical application was evaluated. The most promising areas of further research on the development and application of a new flow cipher in Ukraine are justified.

10 tab. 40 fig. Ref.: 24 items.

СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ
SYSTEMS OF INFORMATION PROCESSING AND PROTECTION

УДК 681.3.06:519.248.681

Аналитическая оценка значений максимальных боковых лепестков функций корреляции сложных нелинейных дискретных сигналов / *И.Д. Горбенко, А.А. Замула* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 76 – 87.

Рассмотрены проблемы синтеза систем нелинейных дискретных сигналов для их использования в информационно-коммуникационных системах (ИКС) в качестве физических переносчиков данных для решения задач обеспечения информационной безопасности и помехозащищенности ИКС в условиях различного рода воздействий со стороны злоумышленника. Предложен метод синтеза систем производных сигналов на основе нелинейных характеристических дискретных сигналов. Представлены результаты исследования свойств данного класса сигналов. Показано, что применение таких систем нелинейных сигналов позволит улучшить показатели информационной безопасности и помехозащищенности.

Табл. 4. Библиогр.: 10 назв.

УДК 681.3.06:519.248.681

Аналітична оцінка значень максимальних бокових пелюсток функцій кореляції складних нелінійних дискретних сигналів / *І.Д. Горбенко, О.А. Замула* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 76 – 87.

Розглянуто проблеми синтезу систем нелінійних дискретних сигналів для їх використання в інформаційно-комунікаційних системах (ІКС) в якості фізичних переносників даних для вирішення завдань забезпечення інформаційної безпеки і завадозахищеності ІКС в умовах різного роду впливів з

боку зловмисника. Запропоновано метод синтезу систем похідних сигналів на основі нелінійних характеристичних дискретних сигналів. Представлено результати дослідження властивостей даного класу сигналів. Показано, що застосування таких систем нелінійних сигналів дозволить поліпшити показники інформаційної безпеки і перешкодозахищеності.

Табл. 5. Бібліогр.: 9 назв.

UDC **681.3.06:519.248.681**

Analytical estimation of the values of the maximum side lobes of correlation functions of complex nonlinear discrete signals / *I.D. Gorbenko, A.A. Zamula* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 76 – 87.

The problems of synthesizing nonlinear discrete signal systems for their use in information and communication systems (ICS) as physical data carriers for solving the problems of information security and noise immunity of ICS in conditions of various kinds of influences on the part of the attacker are considered. A method for synthesizing derived signal systems based on nonlinear characteristic discrete signals is proposed. The results of the investigation of the properties of this class of signals are presented. It is shown that the use of such systems of nonlinear signals will improve the information security and noise immunity.

4 tab. Ref.: 10 items.

УДК 681.3.06

Суперсингулярные полные кривые Эдвардса над простым полем / *А.В. Бессалов, О.В. Цыганкова* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 88 – 98.

Проанализированы условия существования суперсингулярных полных кривых Эдвардса над простым полем. Сформулированы и доказаны три теоремы об условиях существования суперсингулярных кривых с *j*-инвариантами, равными $0, 12^3$ и 66^3.

Ключевые слова: суперсингулярная кривая, полная кривая Эдвардса, скрученная кривая Эдвардса, квадратичная кривая Эдвардса, пара кручения, порядок точки, символ Лежандра, квадратичный вычет, квадратичный невычет.

Табл. 2. Библиогр.: 13 назв.

УДК 681.3.06

Суперсінгулярні повні криві Едвардса над простим полем / *А.В. Бессалов, О.В. Циганкова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 88 – 98.

Проаналізовано умови існування суперсінгулярних повних кривих Едвардса над простим полем. Сформульовано і доведено три теореми про умови існування суперсінгулярних кривих з *j*-інваріантами, рівними $0, 12^3$ и 66^3.

Ключові слова: суперсінгулярна крива, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, пара крутіння, порядок точки, символ Лежандра, квадратичне відрахування, квадратичне невирахування.

Табл. 2. Бібліогр.: 13 назв.

UDC 681.3.06

Supersingular complete Edwards curves over a prime field / *A.V. Bessalov, O.V. Tsygankova* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 88 – 98.

The analysis of the conditions for the existence of super singular complete Edwards curves over a simple field is given. Three theorems are formulated and proved on the conditions for the existence of super singular curves with j-invariants equal to $0, 12^3$ и 66^3.

Keywords: super singular curve, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, torsion pair, order of the point, Legendre symbol, quadratic residue, quadratic non-residue.

2 tab. Ref.: 13 items.

УДК 004.652

Выразительные средства модели данных «объект-событие» / *В.И. Есин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 99 – 112.

Показаны актуальность и важность задачи представления данных при моделировании предметной области. Разработаны выразительные средства (языки концептуального моделирования) для представления концептуальных моделей предметных областей в графическом виде, основанные на модели данных «объект-событие» и являющиеся ее составными элементами. Даны рекомендации по их использованию.

Табл. 2. Ил. 6. Библиогр.: 15 назв.

УДК 004.652

Виразні засоби моделі даних «об'єкт-подія» / *В.І. Єсін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 99 – 112.

Показано актуальність і важливість задачі представлення даних при моделюванні предметної області. Розроблено виразні засоби (мови концептуального моделювання) для подання концептуальних моделей предметних областей в графічному вигляді, засновані на моделі даних «об'єкт-подія» і, які є її складовими елементами. Надано рекомендації по їх використанню.

Табл. 2. Іл. 6. Бібліогр.: 15 назв.

UDC 004.652

Expressive means of the «object-event» data model / *V.I. Yesin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 99 – 112.

The relevance and importance of the problem of data representation in the subject domain modeling are shown. Expressive means (languages of conceptual modeling) are developed to represent conceptual models of subject domains in a graphic form, based on the "object-event" data model and being its constituent elements. Recommendations on their use are given.

2 tab. 6 fig. Ref.: 15 items.

УДК 638.235.231

Обзор проблем безопасности и проектирования защищенных электронных систем / *В.А Горбачев, К.Б. Абдулрахман* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 113 – 119.

Анализируется классификация и методы борьбы с аппаратными закладками (Hardware Trojans). Обосновывается выбор технологии проектирования защищенных ЭС, которая обеспечивает их устойчивость к деструктивному воздействию внутренних компонентов.

Ил. 2. Библиогр.: 19 назв.

УДК 638.235.231

Огляд проблем безпеки та проектування захищених електронних систем / *В.О. Горбачов, К.Б. Абдулрахман* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 113 – 119.

Аналізується класифікація та методи боротьби з апаратними закладками (Hardware Trojans). Обґрунтовується вибір технології проектування захищених ЕС, яка забезпечує їх стійкість до деструктивного впливу внутрішніх компонентів.

Іл. 2. Бібліогр.: 19 назв.

UDC 638.235.231

Overview of security problems and the design of secure electronic systems / *V.A. Gorbachov, K.B. Abdulrahman* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 113 – 119.

The classification and methods of fighting Hardware Trojans are analyzed. The choice of the technology for the design of protected electronic systems is justified, which ensures their resistance to the destructive effect of internal components.

2 fig. Ref.: 19 items.

УДК 004.056.55

Анализ предметной области идентификации и аутентификации / *Д.В. Мялковский, З.А. Орешко, А.В. Потий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 120 – 127.

Работа посвящена анализу терминологии по аутентификации и идентификации, стандартов США, Европейского Союза, международных стандартов ISO / IEC, рекомендации ITU, нормативных документов Украины и национальных стандартов, в том числе гармонизированных с международными.

Табл. 2. Библиогр: 7 назв.

УДК 004.056.55

Аналіз предметної області ідентифікації та автентифікації / *Д.В. Мялковский, З.А. Орєшко, А.В. Потій* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 120 – 127.

Робота присвячена аналізу термінології щодо автентифікації та ідентифікації, стандартів США, Європейського Союзу, міжнародних стандартів ISO/IEC, рекомендації ITU, нормативних документів України та національних стандартів, у тому числі гармонізованих з міжнародними.

Табл. 2. Бібліогр: 7 назв.

UDC 004.056.55

Analysis of domain identification and authentication / *D.V. Mylkovsky, Z.A. Oreshko, A.V. Potii* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 120 – 127.

The work is devoted to the analysis of the terminology of authentication and identification, the standards of the USA, the European Union, international standards ISO / IEC, recommendations of the ITU, normative documents of Ukraine and national standards, including harmonized with international ones.

2 tab. Ref.: 7 items.

УДК 681.142

Методы определения вычетов чисел в комплексной числовой области / *В.А. Краснобаев, А.А. Замула, В.Н. Шлокин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 128 – 142.

Рассмотрены основные методы определения вычетов (остатков) целочисленных данных, представленных в системе остаточных классов (СОК), в комплексной числовой области. Представлены три метода определения вычетов целочисленных данных. Метод определения комплексного вычета целого комплексного числа по комплексному модулю, метод определения наименьшего комплексного вычета целого комплексного числа по комплексному модулю и метод определения вещественного вычета целого комплексного числа по комплексному модулю. Третий метод основан на использовании результатов первой фундаментальной теоремы Гаусса. Приведено множество конкретных примеров определения вычетов целочисленных данных в комплексной числовой области. Результаты исследований целесообразно использовать при обработке комплексных чисел в СОК.

Табл. 5. Библиогр.: 20 назв.

УДК 681.142

Методи визначення лишків чисел в комплексній числовій області / *В.А. Краснобаєв, О.А. Замула, В.Н. Шлокін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 128 – 142.

Розглянуто основні методи визначення лишків цілочисельних даних, представлених в системі залишкових класів (СЗК), в комплексній числовій області. Представлено три метода визначення лишків цілочисельних даних: метод визначення комплексного лишку цілого комплексного числа по комплексному модулю, метод визначення найменшого комплексного лишку цілого комплексного числа по комплексному модулю і метод визначення дійсного лишку цілого комплексного числа по комплексному модулю. Третій метод заснований на використанні результатів першої фундаментальної теореми Гауса. Наведено низку конкретних прикладів визначення лишків цілочисельних даних в комплексній числовий області. Результати досліджень доцільно використовувати при обробці комплексних чисел в СЗК.

Табл. 5. Бібліогр.: 20 назв.

UDC 681.142

Methods of determining the remnants of numbers in a complex numerical domain / *V.A. Krasnobayev, A.A. Zamula, V.N. Shlokin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 128 – 142.

The main methods for determining the residues of integer data presented in the residual class system (SOK) in a complex number area are considered. Three methods for determining the deductions of integer data are presented. Method for determining the complex residue of an integer complex number with respect to a complex modulus, the method for determining the smallest complex residue of an integer complex number with respect to a complex module, and the method for determining the real residue of an integer complex number with respect to a complex module. The third method is based on the results of the first fundamental theorem of Gauss. Many concrete examples of the determination of integers of integer data in a complex number domain are given. The results of the investigations should be used when processing complex numbers in SOK.

5 tab. Ref.: 20 items.

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ
RADIO ENGINEERING AND TELECOMMUNICATIONS NETWORKS AND SYSTEMS

УДК 621.396

Оптимальный алгоритм оценки радияркости в пространственно-распределенных радиометрических системах / *В.К. Волосюк, С. С. Жила, В.В. Павликов, А.Д. Абрамов, В.Г. Яковлев* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 143 – 149.

Выполнена оптимизация обработки шумовых процессов радиотеплового излучения в многоканальных пространственно-распределенных радиометрических системах. Алгоритмы, характерные для применения в системах апертурного синтеза, получены в рамках метода максимального правдоподобия, в предположении, что спектральная яркость излучения в пределах частотной характеристики приемника постоянна, но как изображение излучающего объекта зависит от пространственных (угловых) координат. Особенностью решенных задач является использование спектральных V_F-преобразований, не требующих выполнения условия пространственно-временной узкополосности (квазимонохроматического приближения) и позволяющих решить задачу синтеза алгоритмов обработки широкополосных и сверхширокополосных процессов.

Ил. 1. Библиогр.: 11 назв.

УДК 621.396

Оптимальний алгоритм оцінки радіояскравості у просторово-розподілених радіометричних системах / *В.К. Волосюк, С.С. Жила, В.В. Павліков, О.Д. Абрамов, В.Г. Яковлев //* Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 143 – 149.

Виконано оптимізацію обробки шумових процесів радіотеплового випромінювання в багатоканальних просторово-розподілених радіометричних системах. Отримані алгоритми характерні для застосування в системах апертурного синтезу, отримані в рамках методу максимальної правдоподібності в припущенні, що спектральна яскравість випромінювання в межах частотної характеристики приймача постійна, але як зображення випромінюючого об'єкта залежить від просторових (кутових) координат. Особливістю вирішених завдань є використання спектральних V_F-перетворень, які не потребують виконання умови просторово-часової вузькосмуговості (квазімонохроматичного наближення) і дозволяють вирішити задачу синтезу алгоритмів обробки широкосмугових і надширокосмугових процесів.

Іл. 1. Бібліогр.: 11 назв.

UDC 621.396

Optimal algorithm of radio brightness estimation in the spatial distributed radiometric systems / *V.K. Volosyuk, S.S. Zhyla, V.V. Pavlikov, A.D. Abramov, V.G. Yakovlev //* Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 143 – 149.

Optimization of processing of radio thermal radiation noise processes in multichannel spatially-distributed radiometric systems is performed. The received algorithms applicable in the systems of aperture synthesis are received within the maximum likelihood method in the assumption that spectral brightness of radiation within the frequency band of the receiver is constant, but as the image of a radiating object it depends on spatial (angular) coordinates. Feature of the solved tasks consists in using spectral V_F-transforms which do not require execution of the spatiotemporal band-limitedness (quasi monochromatic approximation) condition and make it possible to solve the problem of synthesis of algorithms for processing wideband and ultra wideband processes.

Fig. 1. Ref.: 11 items.

УДК 621.382(024)

Анализ по показателям качества работы схем узкополосной фильтрации непрерывного доплеровского сигнала / *И.В. Барышев, К.А. Щербина, Е.П. Мсаллам, М.А. Вонсович, А.В. Одокиенко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 150 – 157.

Проведен сравнительный анализ количественных оценок фильтрации по шести показателям качества работы фильтрующих схем непрерывного доплеровского сигнала для систем фазовой

автоподстройки частоты 1-го и 2-го порядка и систем частотной автоподстройки с квадратурно-фазовым частотным дискриминатором со схемой узкополосной фильтрации, реализованной на синхронизированном генераторе с принудительной перестройкой частоты. Средний суммарный показатель выигрыша схемы на синхронизированном генераторе выше остальных в 1,5 раза, а по отдельным показателям – в десятки раз. Разработана методика расчета показателей для схемы фильтрации на синхронизированном генераторе и получены простые расчетные формулы.

Табл.2. Ил. 3. Библиогр.: 13 назв.

УДК 621.382(024)

Аналіз по показниках якості роботи схем вузькосмугової фільтрації безперервного допплерівського сигналу / *І.В. Баришев, К.О. Щербина, Є.П. Мсаллам, М.А. Вонсович, О.В. Одокієнко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 150 – 157.

Проведено порівняльний аналіз кількісних оцінок фільтрації по шести показникам якості роботи фільтруючих схем безперервного доплерівського сигналу для систем фазового автопідстроювання частоти 1-го і 2-го порядків та систем частотного автопідстроювання з квадратурно-фазовим частотним дискримінатором зі схемою вузькосмугової фільтрації, реалізованій на синхронізованому генераторі з примусовою перебудовою частоти. Середній сумарний показник виграшу схем на синхронізованому генераторі вище інших у 1,5 рази, а за окремими показниками – в десятки разів. Розроблено методику розрахунку показників для схем фільтрації на синхронізованому генераторі та отримані прості розрахункові формули.

Табл.2. Іл. 3. Бібліогр.: 13 назв.

UDC 621.382(024)

The experimental research of filtration quality of doppler signal spectral structure by modulated filter / *I.V Baryshev, K.A. Scherbina, E.P. Msallam, M.A. Vonsovitch, A.V. Odokienko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 150 – 157.

The comparative analysis of quantitative assessments of filtering by six performance indices of filter circuits of continuous-wave Doppler signal of 1st order PLL, 2nd order PLL, FLL with narrow-band filter circuit quadrature FM-detector based on synchronized oscillator with forced frequency tuning is carried out. The total average performance indices of the circuit with SG exceeded any of the compared indices by 1.5 times, with a tenfold increase in separate parameters. At the same time the method of indices calculation of filter circuits with SG is developed and simple calculation formulas are obtained.

2 tab. 3 fig. Ref.: 13 items.

УДК 621. 396. 962

Разнесенная двухпозиционная радиометрическая система картографирования объектов / *В.Е. Кудряшев, С. М. Тамаш, Д. С. Шмаков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 158 – 166.

Предложен вариант улучшения чувствительности и разрешающей способности по разности хода в двухпозиционной радиометрической системе (РМС). Приводятся значения радиояркостных температур атмосферного излучения в 3 мм диапазоне длин волн в различных условиях. Получено уравнение дальности действия разнесенной двухпозиционной РМС картографирования поверхности Земли с учетом мешающих радиояркостных температур. Это позволяет обеспечить моделирование РМС в зависимости от ее технических параметров и характеристик малоразмерных объектов. Показано преимущество РМС, если система объект-носитель имеет доплеровскую поправку частоты. Обосновывается вариант уравнения дальности действия разнесенной двухпозиционной РМС для картографирования космических объектов с надземной траектории. Представлены полученные уравнения и графический материал.

Ключевые слова: корреляционный радиометр, радиояркостные температуры, малоразмерный объект, дальность действия, допплеровская поправка частоты, коррелированный фон, полоса картографирования, разрешающая способность по разности хода

Ил. 5. Библиогр.: 23 назв.

УДК 621. 396. 962

Рознесена двохпозиційна радіометрична система картографування об’єктів / *В.Е. Кудряшов, С. М. Тамаш, Д. С. Шмаков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 158 – 166.

Запропоновано варіант поліпшення чутливості та розрізнювальної здатності за різницею хода у двохпозиційний радіометричний системі (РМС). Наводяться значення радіояскравих темпе-

ратур атмосферного випромінювання у 3 мм діапазоні довжин хвиль в різних умовах. Отримано рівняння дальності дії рознесеної двохпозиційної РМС картографування поверхні Землі з врахуванням радіояскравих температур, що заважають. Це дозволяє забезпечити моделювання РМС в залежності від її технічних параметрів та характеристик малорозмірних об'єктів. Показано перевага РМС, якщо система об'єкт – носій має доплерівську поправку частоти. Обґрунтовується варіант рівняння дальності дії рознесеною двопозиційною РМС для картографування космічних об'єктів з надземної траєкторії. Представлені отримані рівняння та графічний матеріал.

Ключові слова: кореляційний радіометр, радіояскраві температури, малорозмірний об'єкт, дальність дії, доплерівська поправка частоти, фон який корельовано, смуга картографування, розрізнювальна здатність за різницею ходу.

Іл. 5. Бібліогр.: 23 назв.

UDC 621. 396. 962

Diversified bi-static radiometric system for object mapping / *V.E. Kudriashov, S.M. Tamash, D.S. Shmakov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 158 – 166.

A variant of improving both the sensitivity and resolution on the path difference in a bi-static radiometric system (RMS) is proposed. Values of the radio brightness temperatures of atmospheric radiation in the 3 mm wavelength band are given in different conditions. An equation is obtained for the range of action of the diversified bi-static RMS for mapping of the Earth surface with allowance for interfering radio brightness temperatures. This makes it possible to provide simulation of the RMS, depending on its technical parameters and characteristics of small-sized objects. The advantage of the BRS is shown for the case in which the Doppler frequency shift is present in the system carriage-target. The variant of the range equation is substantiated at space objects monitoring by orbiting BRS. The obtained equations and figures are presented.

Keywords: correlation radiometer, brightness temperature, small-sized object, range of operation, Doppler frequency shift, correlated background, swath width, time difference of arrival resolution.

5 fig. Ref.: 23 items

УДК 621.391

Исследования методов обнаружения неизвестных сигналов / *В.М. Безрук, С.А. Иваненко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 167 – 172.

Внедрение новых радиосистем ограничивается загруженностью частотных диапазонов и недостаточно эффективным использованием частотного ресурса. Для решения этой задачи была разработана технология когнитивного радио. Для работы данной технологии необходимо применение алгоритмов обнаружения сигналов. Это позволит находить свободные участки спектра с целью их дальнейшего использования. Для работы большинства алгоритмов необходима информация об обнаруживаемых сигналах. На практике это бывает редко. Рассматриваются методы обнаружения неизвестных сигналов, которые не требуют априорных знаний об обнаруживаемых сигналах.

Ил. 3. Библиогр.: 7 назв.

УДК 621.391

Дослідження методів виявлення невідомих сигналів / *В.М. Безрук, С.А. Іваненко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 167 – 172.

Впровадження нових радіосистем обмежується завантаженістю частотних діапазонів і недостатньо ефективним використанням частотного ресурсу. Для вирішення цієї задачі було розроблено технологію когнітивного радіо. Для роботи даної технології необхідне застосування алгоритмів виявлення сигналів. Це дозволить знаходити вільні ділянки спектру, з метою їх подальшого використання. Для роботи більшості алгоритмів необхідна інформація про виявлені сигнали. На практиці це буває рідко. Розглядаються методи виявлення невідомих сигналів, які не вимагають апріорних знань про виявлені сигнали.

Іл. 3. Бібліогр.: 7 назв.

UDC 621.391

Research methods for detecting unknown signals / *V.M. Bezruk, S.A.Ivanenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 167 – 172.

The introduction of new radio systems is limited by the loading of frequency bands and the inefficient use of the frequency resource. To solve this problem the technology of cognitive radio was developed. This technology requires the usage of signal detection algorithms. This will allow finding of free

parts of the spectrum, with the purpose of their further use. However, most of the algorithms require knowledge of certain information about detecting signals. However, in practice this is rare. This paper discusses the methods of detecting of unknown signals, which do not require a priori knowledge of detecting signals.

3 fig. Ref.: 7 items.

УДК 621.396.96:504.064.3

Построение сплошного радиолокационного поля системы гидрометеорологического мониторинга на основе геометрического подхода / *Б.В. Перелыгин, А.М. Лужбин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 173 – 180.

Рассматривается понятие сплошного радиолокационного поля формируемого при помощи системы метеорологических радиолокационных станций. Для размещения метеорологических радиолокационных станций предлагается применять геометрический подход, который заключается в расстановке метеорологических радиолокационных станций в вершинах различных многоугольников и который существенно упрощает построение необходимого радиолокационного поля. Предлагаются количественные показатели для оценки качества радиолокационного поля и приводятся результаты их расчетов для различных вариантов построения радиолокационного поля.

Табл. 2. Ил. 10. Библиогр.: 12 назв.

УДК 621.396.96:504.064.3

Побудова суцільного радіолокаційного поля системи гідрометеорологічного моніторинга на основі геометричного підхода / *Б.В. Перелигін, А.М, Лужбін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 173 – 180.

Розглядається поняття суцільного радіолокаційного поля, яке формується за допомогою системи метеорологічних радіолокаційних станцій. Для розміщення метеорологічних радіолокаційних станцій пропонується застосовувати геометричний підхід, який полягає в розстановці метеорологічних радіолокаційних станцій в вершинах різних багатокутників і який суттєво спрощує побудову потрібного радіолокаційного поля. Пропонуються кількісні показники для оцінки якості радіолокаційного поля та наводяться результати їх розрахунків для різних варіантів побудови радіолокаційного поля.

Табл. 2. Іл. 10. Бібліогр.: 12 назв.

UDC 621.396.96:504.064.3

Construction of a continuous radar field of a hydrometeorological monitoring system based on a geometric approach / *B.V. Perelygin, A.M. Luzbin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 173 – 180.

The concept of a continuous radar field generated by a system of meteorological radars is considered. To accommodate meteorological radars, it is proposed to apply a geometric approach, which consists in arranging meteorological radar stations at the vertices of various polygons and which greatly simplifies the construction of the required radar field. Quantitative indicators for estimating the quality of the radar field and the results of their calculations for various variants of constructing the radar field are proposed.

2 tab. 10 fig. Ref.: 12 items.

УДК 629.7.022

Информационные характеристики звукового излучения малых беспилотных летательных аппаратов / *В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев., О.В. Зубков, М.А.Анохин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 181 – 187.

Приведены результаты сравнения экспериментально полученных информационных характеристик звуковых сигналов двух видов малых беспилотных летательных аппаратов (БПЛА) – квадрокоптера и моноплана. Исследования показали, что энергетические спектры сигналов имеют значительную область широкополосного шума и ярко выраженные гармонические составляющие с частотами, кратными частоте вращения винта. Даже при усреднении спектральных оценок по ансамблю выборок уверенно наблюдаются гармоники с частотами до 8 – 10 кГц. При большом различии режимов двигателей квадрокоптера спектральные максимумы разделяются на несколько, что может являться одним из важных факторов для классификации БПЛА. Описывает-

ся алгоритм оперативного распознавания БПЛА, включающий в себя формирование признаков распознавания на базе спектральных оценок при их ортогональном преобразовании и правило принятия решения на основе критерия Дайса.

Ил. 10. Библиогр.: 10 назв.

УДК 629.7.022

Інформаційні характеристики звукового випромінювання малих безпілотних літальних апаратів / *В.М. Карташов, В.М. Олейніков, С.О. Шейко, С.І. Бабкін, І.В. Коритцев., О.В. Зубков, М.А. Анохін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 181 – 187.

Наведено результати порівняння інформаційних характеристик звукових сигналів, які отримано експериментально для двох видів малих безпілотних літальних апаратів (БПЛА) – квадрокоптера та моноплана. Дослідження показали, що енергетичні спектри сигналів мають значну область широкосмугового шуму та яскраво виражені гармонічні складові з частотами кратними частоті обертання гвинта. Навіть при усередненні спектральних оцінок за ансамблем вибірок упевнено спостерігаються гармоніки з частотами до 8 – 10 кГц. У випадках значної різниці режимів двигунів квадрокоптера спектральні максимуми розділяються на декілька, що може бути одним з важливих факторів для класифікації БПЛА. Описується також алгоритм оперативного розпізнавання БПЛА, який містить в себе формування ознак розпізнавання на базі спектральних оцінок при їх ортогональному перетворенні та правило прийняття рішення на основі критерію Дайса.

Іл. 10. Бібліогр.: 10 назв.

UDC 629.7.02

Information characteristics of sound emission from small unmanned aerial vehicles / *V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V .Zubkov, A.M. Anokhin* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 181 – 187.

The results of comparison of experimentally obtained information characteristics of sound signals of two types of small unmanned aerial vehicles (UAVs) - a quadrocopter and a monoplane are given. Studies have shown that the energy spectra of the signals have a significant region of broadband noise and pronounced harmonic components with frequencies of multiple rotational speeds of the screw. Even with averaging of the spectral estimates for the ensemble of samples, harmonics with frequencies up to 8 ± 10 kHz are confidently observed. With a large difference in the modes of the quadro copter engines, the spectral maxima are divided into severalones, which can be one of the most important factors for the UAV classification. The algorithm for operational recognition of UAV is described, which includes the formation of recognition features on the basis of spectral estimates for their orthogonal transformation and the decision rule based on the Dice criterion.

Fig. 10. Ref.: 10 items.

УДК 621.391

Адаптивный алгоритм перераспределения сетевых ресурсов в сетях с поддержкой технологии NFV / *Хассан Мохамед Мухи-Алдин, Е.Б. Ткачева,* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 188 – 194.

Работа посвящена решению задачи динамического перераспределения сетевых ресурсов в мультисервисных сетях с поддержкой NFV для обеспечения надлежащего уровня качества обслуживания. Решение поставленной задачи достигается за счет разработки адаптивного алгоритма перераспределения сетевых ресурсов, основным критерием которого выступает минимизация конечной стоимости. По результатам математического моделирования проведен эксперимент, который позволил оценить выигрыш от использования разработанного алгоритма.

Табл.1. Ил. 2. Библиогр.: 16 назв.

УДК 621.391

Адаптивний алгоритм перерозподілу мережевих ресурсів в мережах з підтримкою технології NFV / *Хассан Мохамед Мухи-Алдин, О.Б. Ткачова* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 188 – 194.

Роботу присвячено вирішенню задачі динамічного перерозподілу мережевих ресурсів в мультисервісних мережах з підтримкою NFV з метою забезпечення належного рівня якості обслуговування. Рішення задачі досягається за рахунок розробки адаптивного алгоритму перерозподілу мережевих ресурсів, основним критерієм якого виступає мінімізація кінцевої вартості. За резуль-

татами математичного моделювання проведено експеримент, який дозволив оцінити виграш від використання розробленого алгоритму.

Табл.1. Іл. 2. Бібліогр.: 16 назв.

UDC 621.391

Adaptive algorithm reallocation of network resources in a network that supports NFV *TECHNOLOGY / Hassan Mohamed Muhi-Aldeen,* **O.B. TKACHOVA** // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 188 – 194.

The work is devoted to solving the problem of dynamic reallocation of network resources in multi-service networks with the NFV support to ensure an adequate quality of service. This objective is achieved through development of the adaptive network resource reallocation algorithm, the main criterion of which serves to minimize the final cost. Based on the results of mathematical modeling, an experiment was performed that allowed estimating the gain from using the developed algorithm.

Tab 1. Fig.: 2. Ref.: 16 items

УДК 621.38

Частотный преобразователь концентрации газа на основе транзисторной структуры с негативным сопротивлением / *А.В. Осадчук, В С. Осадчук, Я А. Осадчук, Е.А. Селецкая* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 195 – 202.

Представлены частотный преобразователь концентрации газа с резистивным элементом МЕМС MiCS 6814, определяющий концентрацию горючих газов. Рассчитаны и экспериментально подтверждены зависимости активных и реактивных компонентов полного сопротивления преобразователя концентрации газа от напряжений питания и управлении, и от изменения концентрации газа. Получены аналитические выражения для функции преобразования и уравнение чувствительности. Чувствительность преобразователя изменяется от 645 до 175 Гц/ppm в диапазоне значений концентрации от 1 до 1500 ppm и существенно снижается с увеличением концентрации пропана от 1500 ppm до 9000 ppm, и составляет от 175 Гц/ppm до 48 Гц/ppm.

Ил. 10. Библиогр.: 14 назв.

УДК 621.38

Частотний перетворювач концентрації газу на основі транзисторних структур з від'ємним опором / *О.В. Осадчук, В.С. Осадчук, Я.О. Осадчук, О.О. Селецька* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 195 – 202.

Представлено частотний перетворювач концентрації газу з резистивним елементом МЕМС MiCS 6814, що визначає концентрацію горючих газів. Розраховано і експериментально підтверджено залежність активних і реактивних компонентів повного опору перетворювача концентрації газу від напруг живлення та керування і від зміни концентрації газу. Отримано аналітичні вирази для функції перетворення та рівняння чутливості. Чутливість перетворювача змінюється від 645 до 175 Гц / ppm в діапазоні значень концентрації від 1 до 1500 ppm і істотно знижується зі збільшенням концентрації пропану від 1500 ppm до 9000 ppm, та становить від 175 Гц / ppm до 48 Гц / ppm.

Іл. 10. Бібліогр.: 14 назв

UDC 621.38

Frequency converter of gas concentration in transistor structure with negative resistance / *A.V. Osadchuk, V.S. Osadchuk, I.A. Osadchuk, O.O. Seletska* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 195 – 202.

A frequency converter of gas concentration with a resistive element MEMC MiCS 6814, which determines the concentration of combustible gases, is presented. The dependences of the active and reactive components of the impedance of the gas concentration converter on the supply and control voltages and on the change in the gas concentration have been calculated and experimentally confirmed. Analytical expressions for the transformation function and the sensitivity equation are obtained. The sensitivity of the converter varies from 645 to 175 Hz / ppm in the concentration range from 1 to 1500 ppm, and decreases significantly with an increase in the propane concentration from 1500 ppm to 9000 ppm, and is from 175 Hz / ppm to 48 Hz / ppm.

10 fig. Ref.: 14 items.

УДК 534.843.26

Особенности проведения акустического моделирования как завершающего этапа акустической экспертизы помещений зрительных залов на примере драматического театра на 500 мест / *В.В. Усик, И.Г. Мягкий* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 191. – С. 203 – 2011.

Рассмотрен завершающий этап акустической экспертизы зрительного зала на примере драматического театра. На основе результатов, полученных на первых двух этапах, разработаны рекомендации по использованию отделочных материалов для ограждающих поверхностей зала. Проведено моделирование акустических свойств зала в программном пакете Ease 4.4, проанализированы полученные объективные характеристики акустического качества зала.

Табл. 6. Ил. 20. Библиогр.: 9 назв.

УДК 534.843.26

Особливості проведення акустичного моделювання як завершального етапу акустичної експертизи приміщень зали для глядачів на прикладі драматичного театру на 500 місць / *В.В. Усік, І.Г. Мягкий* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 191. – С. 203 – 2011.

Розглянуто завершальний етап акустичної експертизи зали для глядачів на прикладі драматичного театру. На основі результатів, отриманих на перших двох етапах, розроблено рекомендації щодо використання оздоблювальних матеріалів для огороджувальних поверхонь зали. Проведено моделювання акустичних властивостей зали в програмному пакеті Ease 4.4, проаналізовано отримані об'єктивні характеристики акустичної якості зали.

Табл. 6. Іл. 20. Бібліогр.: 9 назв.

UDC 534.843.26

Features of acoustic modeling as the final stage of acoustic examination of premises of auditoriums exemplified by a drama theater for 500 seats / *V. Usik, I. Myagkiy* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №191. – P. 203 – 2011.

The final stage of the acoustic examination of the auditorium is considered on the example of the dramatic theater hall. Based on the results obtained in the first two stages, recommendations are developed on the use of finishing materials for the enclosing surfaces of the hall. The modeling of acoustic properties of the hall in the software package Ease 4.4 is carried out, the received objective characteristics of acoustic quality of the hall are analyzed.

6 tab. 20 fig. Ref.: 9 items.

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 191
Російською, українською та англійською мовами

СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА
Выпуск 191
На русском, украинском и английском языках

Коректор Л.І. Сащенко

Підп. до друку 29.12.2017. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк**.** 11,3. Обл.-вид. арк. 10,77. Тираж 300 прим. Зам. № 221. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.