ISSN 2788-5518

ІНФОКОМУНІКАЦІЙНІ ТА КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ

№ 2(04) 2022

НАУКОВИЙ ЖУРНАЛ

КИЇВ
УНІВЕРСИТЕТ «УКРАЇНА»
2022

ISSN 2788-5518

INFOCOMMUNICATION AND COMPUTER TECHNOLOGIES

№ 2 (04) 2022

SCIENTIFIC JOURNAL

KYIV
UNIVERSITY «UKRAINE»
2022

Засновник, видавець та виробник журналу : «Відкритий міжнародний університет розвитку людини «Україна» .

Свідоцтво про державну реєстрацію:
Серія КВ № 24782-14722 Р від 06.04.2021 р.

Журнал включений до переліку наукових фахових видань ВАК України- категорія «Б» , додаток 4 до наказу МОН України № 735 від 29.06. 2021.

Журнал відповідає вимогам наказу МОН України №32 від 15.01.2018 р.

Має міжнародні коди: ISSN 2788-5518 та DOI 10.36994/2788-5518.

Журнал індексується у міжнародних науковометричних базах Google Scholar , Index Copernicus та каталогах національної бібліотеки України ім. В.І.Вернадського.

Мова видання: українська,англійська

Рекомендовано до друку вченою радою відкритого міжнародного університету розвитку людини «Україна» (протокол № 8 від 18.11.2022 р.)

URL-адреса видання: visn-icct.uu.edu.ua/

Тематика журналу:

- Теоретичні основи інфокомунікацій та комп’ютерних наук
- Інфокомунікаційні системи
- Безпроводові технології
- Технічна електродинаміка та антени
- Волоконно-оптичні системи
- Радіорелейні та супутникові системи
- Телевізійні системи
- Системи відеоконференцзв’яку та відеоспостереження
- Комп'ютерні системи та мережі
- Комп'ютерна і програмна інженерія
- Системи SCADA
- Захист інформації та кібербезпека
- Прикладна математика та моделювання
- Метрологія та інформаційно-вимірювальні системи
- Медична та екологічна електроніка
- Автоматизаія управління технологічними процесам

В журналі публікуються статті для захисту дисертацій зі спеціальностей :121 Інженерія програмного забезпечення.122 Комп’ютерні науки та інформаційні технології.123 Комп’ютерна інженерія.151 Автоматизація та комп’ютерні інтегровані технології .152 Метрологія та інформаційно-вимірювальна техніка.172 Телекомунікації та радіотехніка

Редколегія

Самарай Валерій Петрович, к.т.н., доц., університет «Україна»,
ORCID 0000-0003- 4419-1366, Київ,Україна. *samaraj@ukr.net*

Сидоренко Анатолій Сергійович, д.ф-м.н., проф., академік Академії наук Молдови, ORCID 0000-0001-7433-4140, Кишинів, республіка Молдова. *anatoli.sidorenko@kit.edu*

Стрелковська Ірина Вікторівна, д.т.н., проф., міжнародний гуманіиарний університет, ORCID 0000-0002-1813-0554 , Одеса,Україна. *irina7000370@gmail.com*

Таланчук Петро Михайлович, д. т. н., проф. , університет «Україна»,
ORCID 0000-0001-8748-6127, Київ,Україна. *talanshuk_pm@ukr.net*

Тимошенко Анатолій Григорович, к.т.н, доц., університет «Україна»,
ORCID 0000-0003-0954-3186, Київ,Україна. *timoshag@i.ua*

Ящишін Євген Михайлович, д.т.н., проф., Варшавський технологічний університет, ORCID 0000-0001-8378-1399, Варшава, Польща. *e.jaszczyszyn@ire.pw.edu.pl*

Founder, publisher and producer of the journal: "Open International University of Human Development" Ukraine ".

Certificate of state registration:
Series KV № 24782-14722 R from 06.04.2021.

The journal is included in the list of scientific professional publications of the Higher **Attestation Commission of Ukraine - category "B", Annex 4 to the order of the Ministry of Education and Science of Ukraine № 735 from 29.06. 2021.**

The journal meets the requirements of the order of the Ministry of Education and Science of Ukraine №32 from 15.01.2018.

It has international codes: ISSN 2788-5518 and DOI 10.36994 / 2788-5518.

Publication URL: visn-icct.uu.edu.ua/

Subject journal:
- Theoretical foundations of infocommunications and computer science
- Infocommunication systems
- Wireless technology
- Technical electrodynamics and antennas
- Fiber optic systems
- Radio relay and satellite systems
- Television systems
- Video conferencing and video surveillance systems
- Computer systems and networks
- Computer and software engineering
- SCADA systems
- Information security and cybersecurity
- Applied mathematics and modeling
- Metrology and information-measuring systems
- Medical and environmental electronics
- Automation of process control

Language of publication: Ukrainian, English © University "Ukraine", 2022.

The journal is indexed in international databases and directories of Index Copernicus, Google Scholar, Vernadsky National Library of Ukraine.

Recommended for publication by the Academic Council of the Open International University of Human Development "Ukraine" (Protocol No 8 dated 18.11.2022.)

Publication URL: visn-icct.uu.edu.ua/

Anatoliy Petrenko, Dr. habil., Prof., National technical University of Ukraine "Igor Sikorsky Kyiv polytechnic Institute", ORCID 0000-0001- 6712-7792, Kyiv, Ukraine.*tolja.petrenko@gmail.com*

Valentin Popov, Dr. habil. Phys., Prof., Riga technical University, ORCID 0000-0002-2040-9319. Riga, Latvia. *popovs@latnet.lv*

Vitaliy Pochernyaev, Dr. habil., Prof., University of Intellectual Technologies and Communications, ORCID 0000-0001-7130-8668, Odesa, Ukraine.*vpochernyaev@gmail.com*

Valeriy Rogoza, Dr. habil., Prof., National technical University of Ukraine "Igor Sikorsky Kyiv polytechnic Institute", ORCID 0000-0003-2327-156X Kyiv, Ukraine. *rosvetnik@gmail.com*

Valeriy Samaraj, Ph.D., SSR., University "Ukraine", ORCID 0000-0003-4419-1366, Kyiv, Ukraine. *samaraj@ukr.net*

Anatoliy Sidorenko, Dr. habil. Phys., Prof., Academician of AS of Republic of Moldova, ORCID 0000-0001-7433-4140, Kishinev, Republic of Moldova. *anatoli.sidorenko@kit.edu*

Irina Strelkovskaya, Dr. habil., Prof., International Humanitarian University, ORCID 0000-0002-1813-0554,Odessa, Ukraine. *irina7000370@gmail.com*

Peter Talanchuk, Dr. habil., Prof., University "Ukraine", ORCID 0000-0001-8748-6127, Kyiv, Ukraine. *talanshuk_pm@ukr.net*

Anatoliy Tymoshenko, Ph.D., Ass. Prof., University "Ukraine", ORCID 0000-0003-0954-3186, Kyiv, Ukraine. *timoshag@i.ua*

Eugeniy Yashchyshyn, Dr.habil., Prof., Warsaw University of Technology, ORCID 0000-0001-8378-1399, Warsaw, Poland. *e.jaszczyszyn@ire.pw.edu.pl*

ЗМІСТ

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

CONTENT

INFOCOMMUNICATION TECHNOLOGIES

COMPUTER TECHNOLOGIES

УДК 621.396.969.1

FEATURES OF CODE REDUNDANCY FORMATION IN INFORMATION TRANSMISSION CHANNELS

DOI 10 36994 / 2788- 5518- 2022-02-04-01

Juliy Boiko, *Dr.habil., Prof. Khmelnytskyi National University, Khmelnytskyi, Ukraine. boiko_julius@ ukr.net*

Anatoly Semenko, *Dr.habil.,Prof. Open University of Human Development "Ukraine" , Kyiv, Ukraine.setel@ukr.net*

Ilya Pyatin, *Ph.D., Ass. Prof. Khmelnytskyi Polytechnic Professional College by Lviv Polytechnic National University, Khmelnytskyi, Ukraine. ilkhmel@ukr.net*

Abstract: *The article presents studies of procedures for generating error-correcting codes for various telecommunication technologies. The article is focused on evaluating and identifying mechanisms for adding redundancy to signal-code structures in secure information channels. An important focus of this article is the proposed comparison of the formats of error-correcting codes, the structure of code structures, generator polynomials, code words, and generator matrices. The researches including the analysis of the specifics of inclusion of redundancy in the code structure are given, the general mathematical models of constructive synthesis of error-correcting codes are described. The result is achieved by analyzing convolutional codes, Reed-Solomon codes, turbo codes (TC) and polar codes, which are currently widely used for 5G mobile technology. The verification of the effectiveness of signal-code structures of noise-correcting codes was carried out by the method of mathematical modelling for various telecommunication channels by determining the energy gain of coding (EGC). The performance of the codes was evaluated by establishing a comparison of the coding energy gain for the basic constructions of the codes taken into consideration. It is shown that error-correcting coding is associated with the addition of redundancy. This introduction of redundancy leads to the possibility of eliminating errors in decoding and the resulting error probability at the output of the decoder is reduced compared to uncoded transmission of information in communication channels. The results a study the energy efficiency of turbo codes, convolutional codes, polar codes, low-density parity-check codes, and Reed-Solomon codes are presented. The EGC was about 6 dB. It has been found that enlarging block size of TC, which is decoded, entails appearing of "saturation" effect. For the researched SCC based on TC the values of EGC reached 2 dB for BER level – 10E-4. The possibilities of eliminating the saturation effect of turbo codes using concatenated coding are evaluated. It is assumed that the results proposed in the article will be useful in choosing coding schemes in modern information networks.*

Key words: *telecommunication, encoder, information, error correction, redundancy*

ОСОБЛИВОСТІ ФОРМУВАННЯ КОДОВОЇ НАДЛИШКОВОСТІ У КАНАЛАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Бойко Ю.М*.. д.т.н., проф. Хмельницький національний університет, Хмельницький, Україна. boiko_julius@ ukr.net*

Семенко А.І.*, д.т.н.,проф. Відкритий міжнародний університет розвитку людини «Україна»,Київ, Україна. setel@ukr.net*

П'ятін І.С., *к.т.н.,доц. Хмельницький політехнічний фаховий коледж Національного університету «Львівська політехніка», Хмельницький, Україна. ilkhmel@ukr.net*

Анотація: *В статті представлені дослідження процедур формування кодів з виправлення помилок для різних телекомунікаційних технологій. Стаття зосереджена на оцінці та ідентифікації механізмів додавання надлишковості до сигнально-кодових структур у захищених інформаційних каналах. Наведені дослідження включають аналіз специфіки додавання надлишковості в структуру коду, описано загальні математичні моделі конструктивного синтезу кодів з виправленням помилок. Результат досягається шляхом аналізу згорткових кодів, кодів Ріда-Соломона, турбо-кодів і полярних кодів, які зараз широко використовуються для мобільних технологій 5G. Перевірку ефективності сигнально-кодових конструкцій завадостійких кодів проведено методом математичного моделювання для різних*

телекомунікаційних каналів шляхом визначення енергетичного виграшу кодування.
Ключові слова: *телекомунікації, кодер, інформація, виправлення помилок, надлишковість*

Introduction

The rapid development of telecommunication technologies at the present stage, the introduction of communication standards the fourth (4G) and fifth generations (5G) [1, 2], the development of satellite communications, telemetry systems, etc., poses quite specific tasks for researchers related to ensuring the necessary quality indicators of digital information transmission channels. The important task of ensuring reliable transmission of digital data over different communication channels is more relevant than ever. The solution of this problem lies in the plane of application noise-correcting coding in such channels [3].

It should be noted that the development of telecommunication technologies, the emergence of new digital standards contributes to an increase in the speed of transmission and the volume of transmitted data, and their volume is increasing every year. Naturally, the requirements for the applied codes and methods for their encoding and decoding are increasing. Thus, modern coding systems, in addition to high resistance to interference and reliability in error correction, must have extremely high speeds in data processing [4]. The development of coding theory allows us to state that an effective direction in the construction of decoder circuits is the direction associated with the use of a significant number of high-speed elements of microelectronics. In this case, it is expedient to refuse from long feedback channels, which directly affect the reduction in the rate of data transmission advancement. In addition, the implementation of decoding schemes should, if possible, avoid the situation when the number of calculations per decoded symbol turns out to be a random variable, and more complex decoder schemes should be built to perform efficient decoding [5].

Coding theory is an applied science [3, 5]. It is integrated into the tasks being solved, including means of telecommunications, radar, measuring, computing and control equipment. In this case, the fact of the possibility of applying the obtained results, their competitiveness in comparison with non-coded methods of error protection is of great importance. Practical achievements of coding theory are now well known [6]. However, the most widely used at the present stage of development of telecommunication technologies are such coding methods as convolutional codes (CC), Reed-Solomon codes (RS), turbo codes (TC), low-density parity codes (LDPC) [1], polar codes (PC), which became the basis for the deployment of 5G mobile telecommunications [7-10].

Application of spectrally effective modulation methods, effective coding methods, in particular signal coding construction (SCC), creates preconditions to research basic parameters of signal processing systems, telecommunication systems and optimize data decoding algorithms. The actual problem here is in finding noise immunity for modulation methods, benefits from coding, energy gain, symbol error probability benefits for receiver, acceptable code redundancy, complexity and rate of codec and synchronizing received signals. Conception of improving noise immunity in telecommunication systems, that belong to 4th and 5th generations [10, 11] and are used in conditions of high noise and hindrances becomes actual for communication systems developers, especially when data transmission standards are rapidly rising and taking into account the world trends and requirements to operation of data processing devices [12].

Noise-immune coding is necessarily associated with the introduction of symbol redundancy, which, in the case of a constant information source rate, leads to a decrease in the duration of the symbols and, for a constant transmitter power, to a decrease in the energy that falls on one symbol. It should be noted that in this case the probability of error increases. However, due to error correction during decoding, the resulting error probability at the output of the decoder will be less than in the case of uncoded transmission of information. An important indicator of coding efficiency is the energy gain resulting from coding (EGC) [4], which is generally determined through the difference between the signal-to-noise ratios in the case of uncoded and coded transmission, provided that the same bit error probability in the channel is provided.

Thus, the proposed article presents the problem of analyzing the principles of the formation of redundancy in error-correcting codes. For analysis, the above codes are taken - convolutional,

Reed-Solomon, turbo codes and polar codes. As a result of the analysis, it is necessary to obtain generalized principles for constructing codes, as well as comparative characteristics of codes for different degrees of redundancy. The subject of the research of the article is the methods and means ensuring the noise immunity telecommunication systems of information transmission based on the definition the structure of the code structure. The paper describes a set of scientifically based theoretical provisions, as well as practical recommendations and proposals for the development of mechanisms for a formalized description of a methodology for increasing the efficiency of coding / decoding in telecommunication information transmission systems.

Theoretical Description

Error Correction Codes (ECC) are a sequence of numbers generated by special algorithms to detect and correct errors in data transmitted over noisy channels. Error correction codes identify corrupted bits and their location.

Let's start with convolutional codes.

In convolutional codes, the input bits are not divided into blocks, but are transmitted as bit streams, which are convolved into the original bits based on the logic function of the encoder. Also, in convolutional codes, the source stream depends not only on the current input bits, but also on the previous input bits stored in memory.

To generate a convolutional code (CC), information is sequentially passed through a linear shift register with a finite number of states. The shift register consists of (bit) stages and logic function generators. The convolutional code can be represented as (*n, k, K*), where:

- *k* - the number of bits shifted in the encoder at one time. Usually, *k* = 1;
- *n* - the number of encoder output bits corresponding to *k* information bits:
- *K* is the number of states of the shift register;
- Code rate, $R_c = k/n$;
- the sequence of input bits is transmitted to the encoder sequentially, starting from the last bit of the block.

Convolution code generation example is presented in fig. 1. Consider a convolutional encoder with *k*=1, *n*=2 and *K*=3. Code rate: $R_c = k/n = 1/2$.

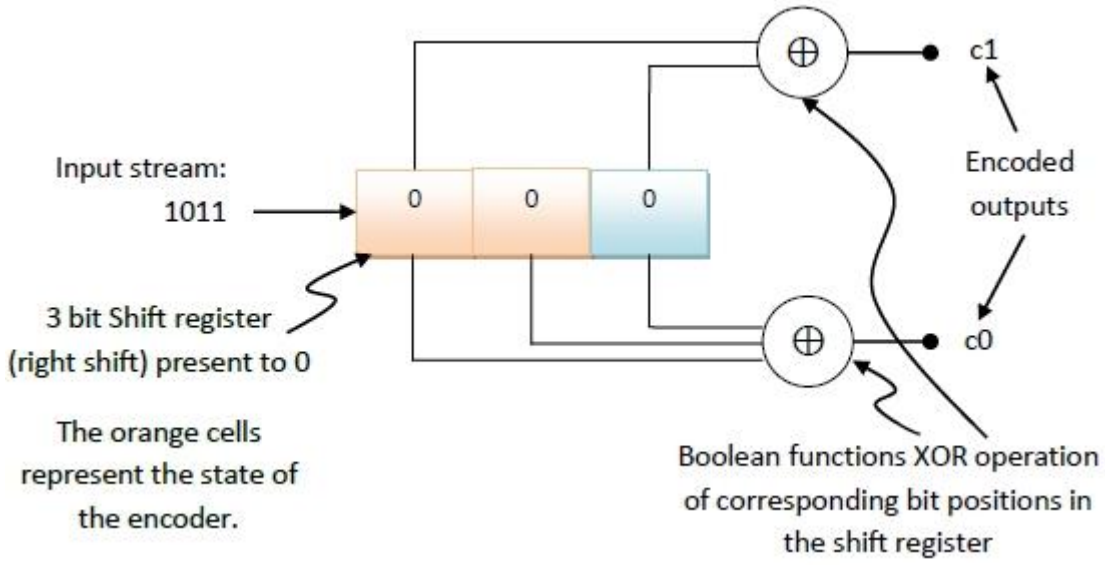


Fig. 1. Convolution code generation

The value of the bits at the output of the convolutional encoder is calculated by the logical function "exclusive OR" (modulo 2 additions, XOR), which has the following graphic symbol and truth table 1:

For the XOR function, a unit at the output of a logic element appears when only one is active at one input. If there are two or more units at the input, or zero at all inputs, then the output will be zero. The change in the state of the registers and the signal at the outputs of the encoder, depending on the input information sequence, is shown in table 2.

Table 1. Truth table

INPUT X1	INPUT X2	OUTPUT Y
0	0	0
1	0	1
0	1	1
1	1	0

Table2.

Changing the state of the registers and the signal at the outputs of the encoder depending on the input information sequence

SHIFT REGISTER STATUS	OUTPUT C1	OUTPUT C0
$b1\ \ b2\ \ b3$	$b1 \oplus b3$	$b1 \oplus b2 \oplus b3$
0 0 0	0	0
1 0 0	1	1
1 1 0	1	0
0 1 1	1	0
1 0 1	0	0

That is, if the input sequence is: 1 0 1 1

The output will be the sequence: 0 0 1 0 1 0 1 1.

Now let's consider how redundancy is formed in Reed-Solomon codes.

Unlike coding with "soft decision" used for convolution codes (CC), the output of decoder RS is "hard", so decoder acts on alphabets symbol that is used in coding. Noteworthy is that decoder RS creates undistorted sequence in the output if received sequence of symbols differ from the real word by t symbols maximally [5]. Decoder automatically detects information on number of errors. In forward error correction system, the RS code (255, 239) will be used that is highly effective in the packet error medium. The code construction consists of: code word length n=255 bytes; number of information symbols in data block k=239 bytes; number of errors fixed in code word $t=(n-k)/2=8$; number of errors detected in code word $2 \cdot t$ =16. Fig. 2 represents RS code (255, 239) construction.

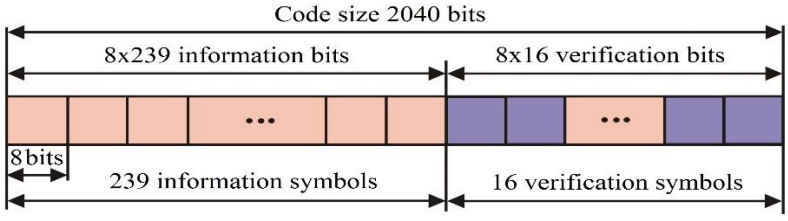


Fig. 2. Reed-Solomon code (255, 239) construction

In error correction scheme codec processes data block (information bytes 1...239) and calculates verification symbols (bytes 240...255), fig. 3.

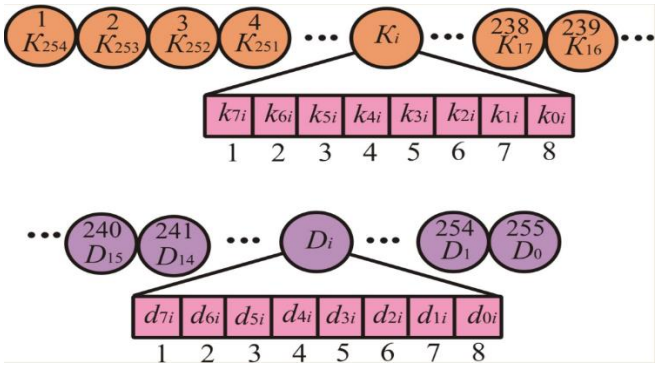


Fig. 3. Code word construction for coding with noise immunity and error correction

Bytes that belong to code word x are represented as:

$$x + 16(j-1), j = 1\ldots255\ . \tag{1}$$

The generator polynomial is represented as:

$$G(z) = \prod_{i=0}^{15}(z - \alpha^i), \tag{2}$$

where α – root of binary primitive polynomial of type: $x^8 + x^4 + x^3 + x^2 + 1$.

The code word construction will be represented by polynomial as:

$$Y(z) = K(z) + D(z) \tag{3}$$

that is a summation of information and verification bytes, Fig. 4.

Information bytes will be represented by the polynomial:

$$K(z) = K_{254} \cdot z^{254} + K_{253} \cdot z^{253} + \ldots + K_{16} \cdot z^{16}\ , \tag{4}$$

where $K_j (j = 16\ldots254)$ – information byte given by element of the Galois field GF(256), then $K_j = k_{7j} \cdot \alpha^7 + k_{6j} \cdot \alpha^6 + \ldots + k_{1j} \cdot \alpha^1 + k_{0j}$.

Such construction is described by: bit k_{7j} – most significant bit, and k_{0j} – least significant bit; byte K_{254} – corresponds to first byte in code word, and K_{16} – 239.

The pairing verification bytes are represented as:

$$D(z) = D_{15j} \cdot z^{15} + D_{14} \cdot z^{14} + \ldots + D_1 \cdot z^1 + D_0 \tag{5}$$

where D_j (j =0…15 – verification byte given by element of the Galois field GF(2^8) and $D_j = d_{7j} \cdot \alpha^7 + d_{6j} \cdot \alpha^6 + \ldots + d_{1j} \cdot \alpha^1 + d_{0j}$.

Bit d_{7j} is most significant bit, d_{0j} – least significant bit of pairing verification byte. Byte corresponds to byte 240 of under-feed which is responsible for coding with forward error correction (FEC) and byte R_0 corresponds to byte 255.

The verification bytes $D(z)$ will be calculated as:

$$D(z) = K(z)\, mod\, Y\,(z), \tag{6}$$

where mod – module calculated by generator polynomial $Y(z)$ with elements of GF(2^8). Each element in Galois field GF(2^8) will be determined by primitive polynomial: $x^8 + \mathrm{x}^4 + \mathrm{x}^3 + \mathrm{x}^2 + 1$. Hemming distance of RS code (255, 239) – d_{min} [5].

In error correction mode code can correct up to 8 errors of symbols in code word FEC and can detect up to 16 errors of symbols in code word FEC on error detection mode [1].

Coding is performed with reverse Fourier transform:

$$c_j^{/} = C(z^j) \quad , \tag{7}$$

where z=2 – primitive element of the field.

Conditions to be considered are: forming SCC requires identification which elements are informational and which are verifying (redundant). Mention was made that number of redundant symbols should be twice higher than the number of error symbols which should be renewed. If the double error is to be corrected (t = 2 – error multiplicity), then four verification symbols should be used correspondently.

Decoding is conducted by the formula:

$$c_j = C^{/}(z^{-j}) \tag{8}$$

Counting redundant symbols is sufficient to verify if information is not distorted. If their number equals zero then errors are absent. To correct an error, first of all, the position of error symbol should be defined. This requires calculation of error locator's polynomial whose roots will point to error positions. The locator polynomial is represented by matrix as: L = [1, l_1, l_2, ... l_t].

Matrix and vector-column will be formed, which is required for calculation of error locators L. This process is formalized as:

$$G = \begin{pmatrix} S_{t-1} & \dots & S_1 & S_0 \\ & \dots & & \\ S_{2t-2} & & S_t & S_{t-1} \end{pmatrix}, \qquad \begin{pmatrix} l_1 \\ \dots \\ l_t \end{pmatrix} = G^{-1} \cdot J,$$
$$J = \begin{pmatrix} S_{t-2} \\ \dots \\ S_{2t-2} \end{pmatrix}. \tag{9}$$

The reverse matrix G^{-1} will be calculated taking into account calculation rules in the Galois field. Summarizing error vector with distorted code sequence will result in correct coded sequence whose decoding will deliver correct information symbols.

Coder presents digital machine where all operations are performed in the Galois field by module of primitive polynomial. The information in byte form is incoming to codec's input. Information symbols are going to codec's output with no delay in case of switches P1 and P2 are in position 1. After k information symbols come, codec's input switches off, P1 and P2 are in position 2 and $n - k$ verification symbols, which are contained in the shift registers (fig. 4), are coming to the output.

The represented coder scheme is specific in having N registers. In the scheme the principle of block interleaving is used, which can be described by matrix of X rows and Y columns. In this case data is read by columns in transmitter and by the rows in the receiver. Parameter Y equals to the length of code word in block code. The advantage is obtained by: since RS code coding gives block length multiple of X·Y, the scheme is obtained, in which register cleaning process is absent.

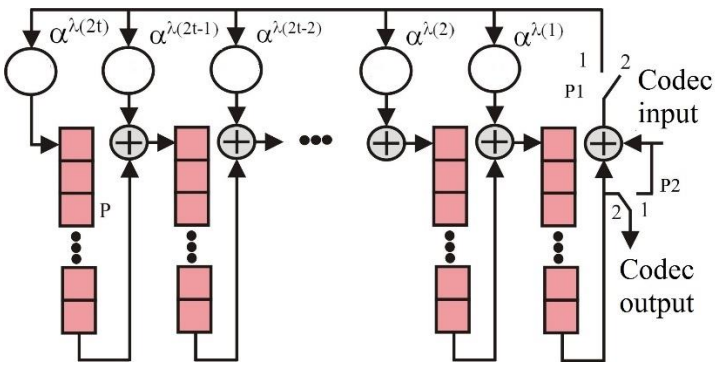


Fig. 4. RS coder scheme with interleaving data: R – shift register; P - switches; α – Galois field

element

Such scheme redundancy, which is due to presence of interleaver, will be zero. Scheme of such coder cyclically processes input information sequence in form of bytes.

The general structure of the frame used in channel coding is shown in fig. 5.

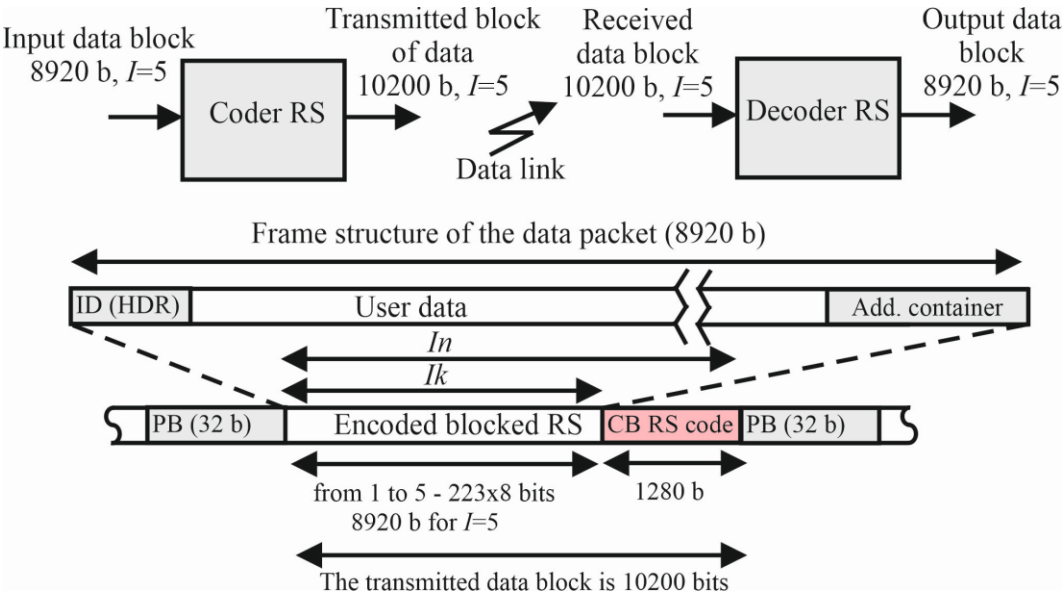


Fig. 5. Frame structure of a data packet for transmitting information by the RS code: ID - the name of the input frame data (header); PB - check bits; CB - synchronization control bits, *I*=5 - interleaver length

Let us now consider the principles of redundancy formation in the design of TC.

The code word is represented by 16-bit construction of Hemming block code (16, 11). Such code contains 11 information bits and 5 verification ones, fig. 6.

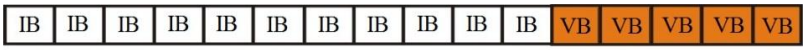


Fig. 6. Code word to build turbo-code: IB – information bits; VB – verification bits

Fig. 7 demonstrates results of building TC as two-dimensional construction 16x16 bits. The turbo-code synthesis is represented by the following sequence. The matrix is formed whose base is made of 11 input bits: matrix 16x11 and verification bits.

Noteworthy is that in matrix cells, shown in Fig. 6, various codes can be used: Hemming, Golay and others. Vertical blocks in code word can be built with Golay code, and horizontal ones – with Hemming code for an instance. Then we obviously obtain two-dimensional turbo-code.

Fig. 8 demonstrates process of building turbo-code as three-dimensional construction. To correct productivity of turbo-code decoder considered in the decoder is offered to be improved by including scaling block. The idea is that outer information is multiplied by the specified scale before it is put again in the input of component decoder through the scheme of iterative decoder.

Fig. 9 shows the simulation scheme of decoder construction described above. Simulation is conducted within the research framework of telecommunication system for transmitting data with turbo-coding.

The scheme can be divided into APP-decoder, interleaving blocks, scaling sub-system – Scaling. The logarithmic ratio of likelihood functions for each information symbol u_l is represented as:

$$G(u_l) = ln\left[\frac{p(u_l=+1)}{p(u_l=-1)}\right] \cdot k_{м1}\ , \qquad (10)$$

where $p(u_l = n)$ – event probability $u_l = n$ and $u_l = n$.

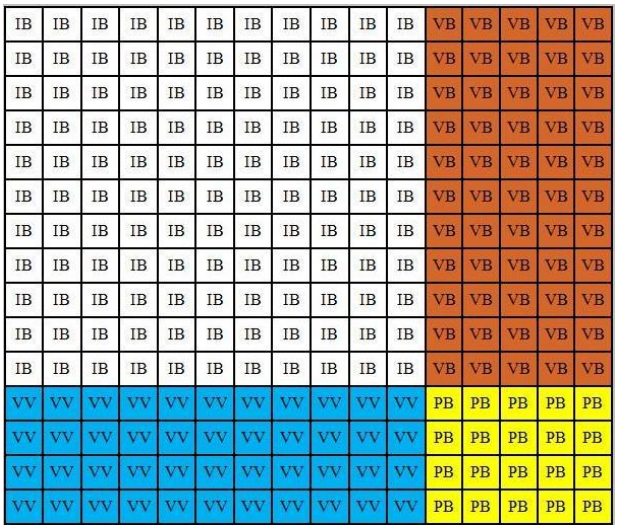


Fig. 7. Code word for building two-dimensional turbo-code: VV – vertical verification bits; PB – pre-implementation verification bits

Decoder SISO1 (Inner Decoder) on the base of information received from transmission channel assesses information bits with account for scale. Then outer information is formed from made assessment $G(u_k^{/}|\overline{y})$ with account for scale by excluding a priori information and systematic symbols received from the channel. This process is formalized as:

$$G_{\text{зв}}^{/}(u_l) = G(u_l^{/}|\overline{y}) - G_a y_{ls} - G(u_l), \tag{11}$$

where for discrete Gaussian channel without memory (AWGN) member $G_a = 2/\sigma^2$ will determine channel reliability, and σ^2 – noise dispersion.

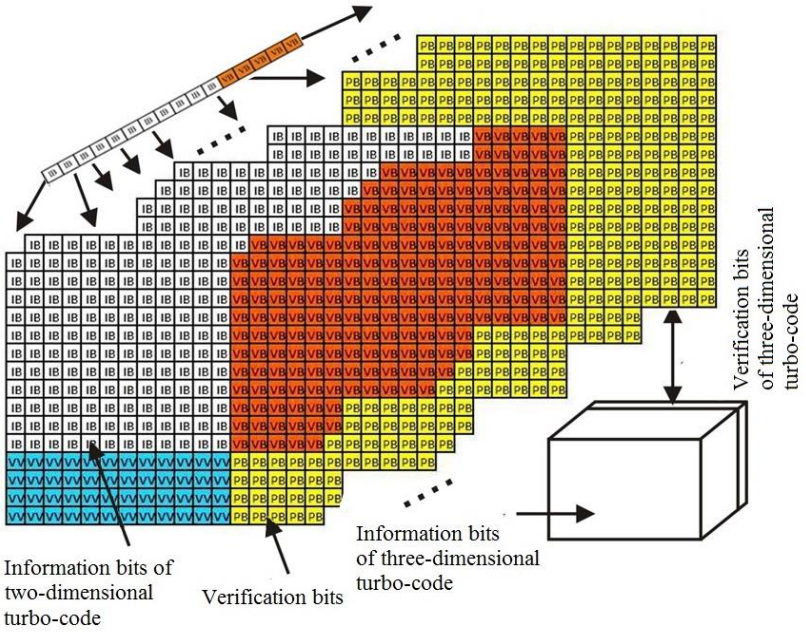


Fig. 8. Code word for building three-dimensional turbo-code: VB – verification bits of three-dimensional realization

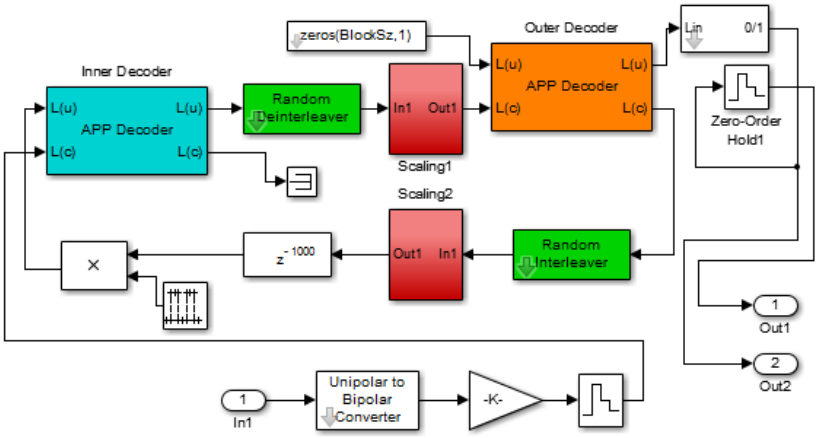


Fig. 9. The frame of subsystem simulation scheme for turbo-code decoder

Second SISO2 (Outer Decoder) uses received information (a priori) for self-assessment with account for scale $k_{\text{м2}}$.

For Gaussian channel, in which noise has zero mean value and dispersion σ^2, when a priori probability is replaced for probability density function, the following expression will be obtained:

$$\Lambda(\hat{d_k}) = \pi_k \exp\left(\frac{2x_k}{\sigma^2}\right) \frac{\sum_m \alpha_k^m \exp\left(\frac{y_k v_k^{i,m}}{\sigma^2}\right) \beta_{k+1}^{f(1,m)}}{\sum_m \alpha_k^m \exp\left(\frac{y_k v_k^{0,m}}{\sigma^2}\right) \beta_{k+1}^{f(0,m)}} = \pi_k \exp\left(\frac{2x_k}{\sigma^2}\right) \pi_k^e , \quad (12)$$

where $\pi_k = \pi_k^{/} / \pi_k^0$ – will be input ratio of a priori probabilities (a priori likelihood), and π_k^e – outer output likelihood received in a moment k – correction (correction member) of coding, which changes input priori information of data bits. In turbo-code such correction members pass from one decoder to another in order to improve ratio of likelihood functions for each information bit and in such way to minimize decoding error probability. Thus, decoding process is followed by using equation (12) to obtain several iterations $\Lambda(\hat{d_k})$. Outer likelihood π_k^e obtained from concrete iteration substitutes a priori likelihood π_{k+1} for the next iteration.

TS and convolutional codes are typical for use in 4G telecommunications. Consider the principles of redundancy formation for the code that is typical for 5G [9].

Consider a polar code encoder with *N*=4 bits input. The polar code of this data vector is calculated by the expression: $x_1^N = u_1^N G_N$. Here x_1^N, is a code vector containing *N* bits. G_N is a generator matrix and is calculated by the expression: $G_N = B_N F^{\otimes n}$. *F* is the Kronecker matrix. The matrix B_N is calculated using the following expression: $B_N = R_N(I_2 \otimes B_{N/2})$. R_N is the permutation operator. I_2 - information array. A polar encoder of a 4-bit long data vector is shown in the Fig. 10 below.

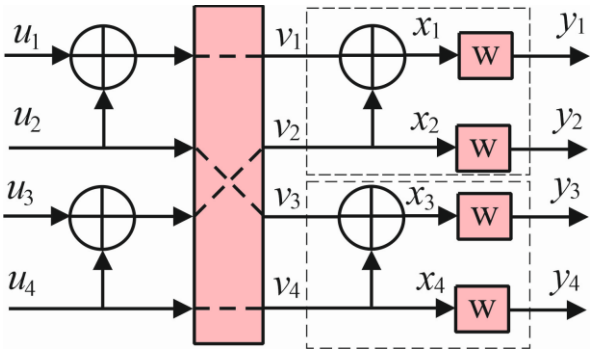


Fig. 10. Polar coding scheme

Consider an example of how a polar encoder works without moving. Let: *K*=132 – informational message length; *E*=256 is the length of the rate-matched output block [13].

Next comes the construction of the polar encoder. The MATLAB function returns an *N*-bit vector (*N*=256) as the original data, where the K elements in the original data will be 0 (the location of the information bits. *K*=132), and the *N-K* elements in the original data will be 1 (frozen bits). positions *N–K*=124). *E* is the length of the output at the agreed rate, and N_{MAX} is the maximum value of *n* (9 or 10). The code rate is defined as *K/E*.

As a result of constructing the encoder, indexes of the location of frozen bits and parity bits are determined.

Next, the generator matrix *G* is defined as the nth order of the products of the Kronecker matrix [13], *n*=8:

.

$$G = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \quad . \tag{13}$$

As a result, the matrix *G* will have dimensions of 256×256 elements.

For polar coding, the mod 2 product operation of the generator matrix and the input data array is performed.

Below we present the MATLAB program code designed to generate polar codes.

MATLAB code for polar encoding CRC-Aided Polar.

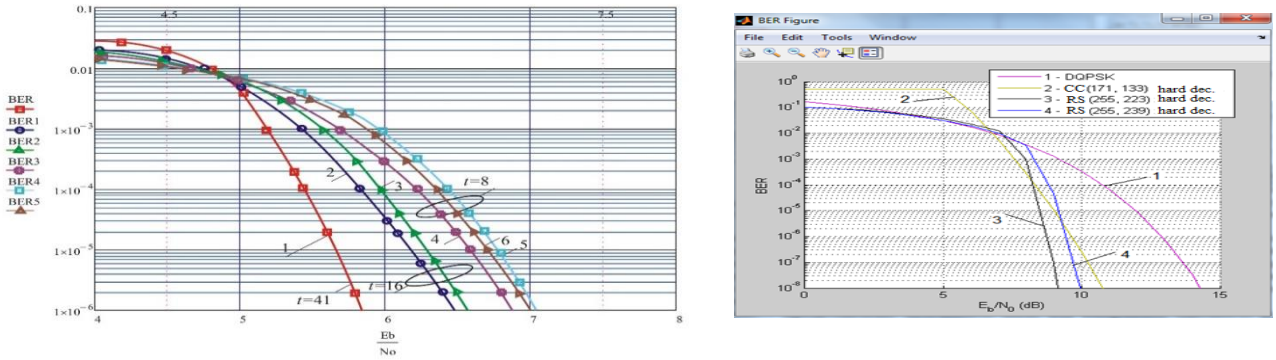
```
K = 132;           % Message length
E = 256;           % Rate matched output length 256
in = randi([0 1],K,1);              % Generate random message
nMax = 10;       % maximum n value for N
iIL = false;     % input interleaving
out1 = nrPolarEncode(in,E,nMax,iIL);           % Polar encode
% Get frozen bit indices and parity-check bit locations
   [F,qPC] = nr5g.internal.polar.construct(K,E,nMax);
   N = length(F);
   nPC = length(qPC);
      inIntr = in;
   % Generate u
   u = zeros(N,1);     % doubles only
      % CRC-Aided Polar (CA-Polar)
      u(F==0) = inIntr;   % Set information bits (interleaved)
   % Get G, nth Kronecker power of kernel
   n = log2(N);
   ak0 = [1 0; 1 1];   % Arikan's kernel
   allG = cell(n,1);   % Initialize cells
   for i = 1:n
      allG{i} = zeros(2^i,2^i);
   end
   allG{1} = ak0;      % Assign cells
   for i = 1:n-1
      allG{i+1} = kron(allG{i},ak0);
   end
   G = allG{n};
   % Encode using matrix multiplication
   outd = mod(u'*G,2)';
   out = cast(outd,class(in));
```

Estimation of Encoding Gain

This section presents the experimental results of performance evaluation of various error-correcting codes. The noise immunity was evaluated by determining the energetic coding gain, the method for obtaining which is described above in the text of the article. This assessment is rather arbitrary. First of all, as described in the article, a certain signal-code constructing (SCC) finds application in a certain

telecommunication technology for solving specific buildings. In this case, the structure of the error-correcting code, the requirements for its noise immunity, the main indicators: code rate, redundancy, degree of interleaving, degree of puncturing, and others, will differ significantly. However, the invariance with respect to certain parameters of the SCC will make it possible to obtain a certain, general graph of noise immunity. Such a graph will make it possible to assess in general the possibilities of the codes taken for consideration in terms of energy efficiency, approaching the Shannon boundary. This is the essence of the results presented in this section.

Fig. 11 shows the dependencies of BER on the corrective ability of RS codes. In particular, the simulation results make it possible to establish that the code RS (255, 173) has the best performance in the case of *t*=41.



a b

Fig. 11. Dependencies for assessing the noise immunity of RS codes: a - 1 - (255, 173); 2- (157, 125) 3 - (255, 223), 4 - (97, 81), 5 - (255, 239); 6 - (204, 188); b - to determine the energy gain of coding

Unlike the "soft" decisions used for convolutional codes, the output of the RS decoder is "hard" so that the decoder acts on the character of the alphabet that is used in the encoding. It is important to note here that the RS code decoder creates an undistorted sequence at the output if the sequence of received symbols differs from the real word by no more than t symbols, which was shown in [4]. In this case, the decoder automatically sets the information about the number of errors.

On Fig. 12 and Fig. 13 shows the results of the study of noise immunity for concatenated codes according to the SCC: RS(255, 223)+CC and RS(255, 239)+CC and convolutional codes.

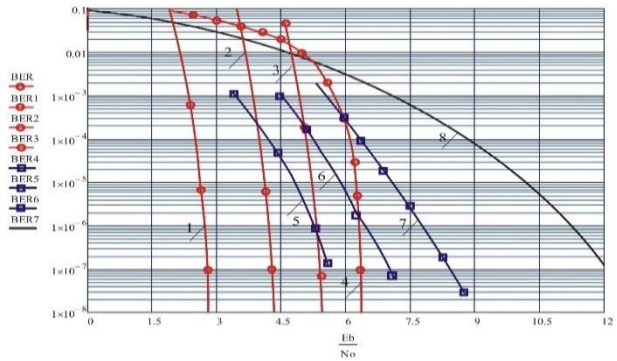


Fig.12. Plots of BER from (E_b/N_0) for convolutional and concatenated code at different coding rates at: *t*=16: 1 - RS+CC(255, 223), *R*=1/2 ; 2- RS+CC(255, 223), *R*=3/4, 3- RS+CC(255, 223), *R*=7/8; 4 - RS(255, 223); 5 – CC *R*=1/2; 6- CC *R*=3/4; 7- CC, *R*=7/8; 8- uncoded QPSK

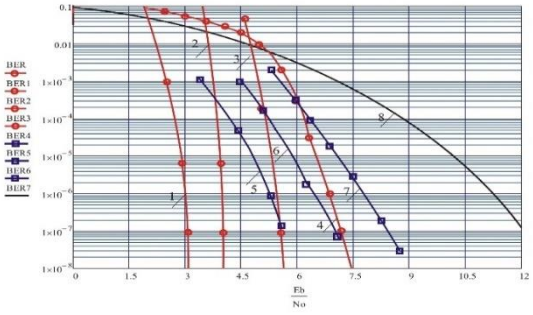


Fig.13. Plots of BER from (E_b/N_0) for convolutional and concatenated code at different coding rates at: *t*=8: 1 - RS+CC(255, 239), *R*=1/2 ; 2 - RS+CC(255, 239), *R*=3/4, 3- RS+CC(255, 239), *R*=7/8; 4 - RS(255, 239); 5 – CC *R*=1/2; 6 - 3К, *R*=3/4; 7 - CC *R*=7/8; 8 - uncoded QPSK

The results of the study allow us to establish that the efficiency of using concatenated codes is higher than when using RS codes separately (compare, for example, Fig. 12, 1 and Fig. 12,

5, the energy gain is almost 3.2 dB (BER=10E-7).

Let's consider how the number of iterations affects the decoding efficiency and noise immunity of turbo codes. Used turbo code: TC $(7, 5)_8$ with rate R=1/2 with puncturing (perforated code), frame length for interleaving I=400 bits. Decoding was performed according to the log-MAY algorithm. On fig. Fig. 14 shows the dependence of the error probability on that obtained in the simulation. The axes are, respectively, the bit error probability (BER), the signal-to-noise ratio in dB, and the number of iterations during decoding. The simulation result is a surface formed by sections, each of which determines the dependence of the bit error probability on a fixed number of iterations. An analysis of the graph allows us to establish the following: code characteristics and noise immunity improve with an increase in the number of iterations, however, after the seventh iteration, this improvement is rather insignificant. We use the proposed modified SCC: RS (255, 223) + TC (I = 16384 bits; 15 iterations) + DQPSK and present noise immunity graphs. Decoding was performed using the log-MAP algorithm (fig. 15).

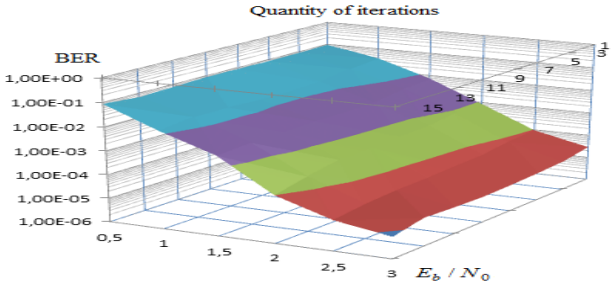


Fig.14. Dependences of noise immunity for the proposed TC on the number of iterations

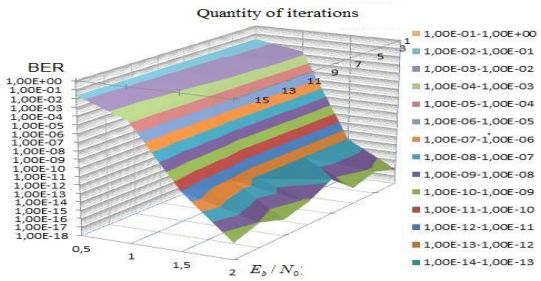


Fig.15. Noise immunity dependences for the offered SCC in case of changing iteration quantity in TC

The offered scheme has removed TC saturation effect for the offered codes and allowed to obtain EGC at the level of 3.1 dB (BER=10E-8)

In order to compare the codes described above in the article, we determined the performance of the RS, CC, LDPC (Low-density parity-check code) [9], TC and polar codes. Mathematical modeling used SCC with QPSK, code rate 2/3,fig.16.

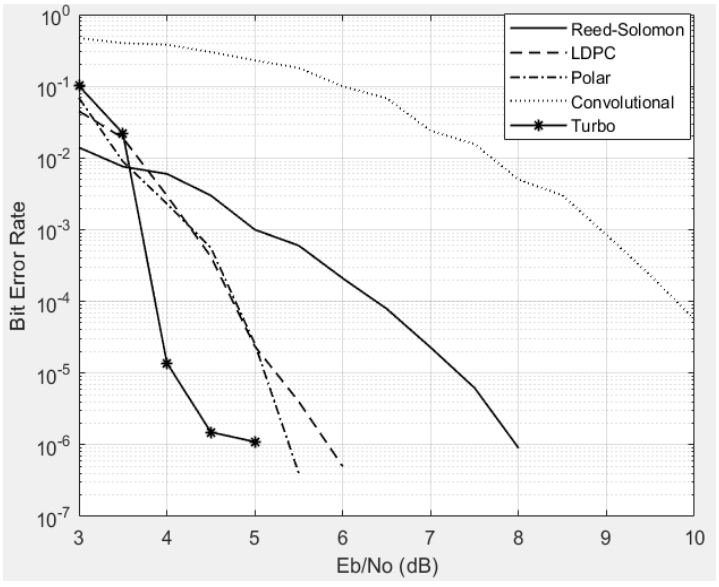


Fig.16. Noise Immunity Graph to Compare Energy Efficiency of CC, TC, RS, Polar Code and LDPC

Conclusions

The conditions for increasing the spectral and energy efficiency when establishing the evaluation requirements for digital telecommunications transmission systems are determined. The analysis noise-immune coding algorithms in telecommunication systems of information transmission is carried out. The features the implementation of noise-immune coding algorithms

in telecommunication channels information transmission with digital modulation types are considered. The features of the use error-correcting codes in digital telecommunication systems for information transmission are determined. Practical recommendations are given on the structure, redundancy and form of SCC in solving the problem increasing the noise immunity of information transmission under conditions of a real interference complex.

Література

1. Пятін І., Бойко Ю. Порівняння продуктивності завадостійких кодів на основі програмного HDL моделювання для захищених інформаційних технологій. *Інфокомунікаційні та комп'ютерні технології*, 2022. № 1(03). С. 43-68.
2. Bioglio V., Condo C., Land I. Design of Polar Codes in 5G New Radio. *IEEE Communications Surveys & Tutorials*, 2020. P. 1.
3. Dumas J-G., Roch J-L., Tannier E., Varrette S. Error Detection and Correction. Foundations of Coding: Compression, Encryption, Error Correction. Wiley, 2015. P.209-276.
4. Boiko, J., Pyatin, I., Eromenko, O., Stepanov, M. Method of the adaptive decoding of self-orthogonal codes in telecommunication. *Indonesian Journal of Electrical Engineering and Computer Science*. 2020. №19(3), P. 1287-1296.
5. Kim H. Error Correction Codes. Wireless Communications Systems Design. Wiley, 2015, P.123-207.
6. Berkman L., Turovsky O., Kyrpach L., Varfolomeeva O., Dmytrenko V., Pokotylo O. Analyzing the code structures of multidimensional signals for a continuous information transmission channel. *Eastern-European Journal of Enterprise Technologies*, 2021.Vol. 5, № 9. P. 70–81.
7. Семенко А.І., Кушнір М. Я., Бокла Н. І. Синтез широкосмугової телекомунікаційної системи з підвищеною конфіденційністю передачі інформації шляхом використання псевдовипадкових послідовностей на основі хаосу. *Вісник університету «Україна». Серія: інформатика, обчислювальна техніка та кібернетика*, 2020. №1(24). С.65-75.
8. Бірюков, М., Семенко, А., Тріска, Н. Принципи узгодження цифрових потоків транспортних телекомунікаційних мереж. *Інфокомунікаційні та комп'ютерні технології*, 2021. № 2(02). С. 64-80.
9. Boiko, J., Pyatin, I., & Eromenko, O. Design and Evaluation of the Efficiency of Channel Coding LDPC Codes for 5G Information Technology. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, 2021. № 9(4), P. 867-879.
10. Бойко, Ю., П'ятін, І., Карпова, Л., Пархомей, І. Transmission of control information in 5G broadband telecommunication systems. *Адаптивні системи автоматичного управління*, 2021. №1(38), С. 82-95.
11. Luo F. Deep Learning Techniques for Decoding Polar Codes. *Machine Learning for Future Wireless Communications*. 2020., P.287-301.
12. Bae J., Abotabl A., Lin H., Song K., Lee J. An overview of channel coding for 5G NR cellular communications *APSIPA Transactions on Signal and Information Processing*. 2019, No. 8, E17.
13. Arikan E. Systematic Polar Coding*. IEEE Communications Letters*. 2011. Vol. 15, No. 8. P. 860-862.

References

1. Pyatin, I., Boiko, J. (Porivniannia produktyvnosti zavadostiikykh kodiv na osnovi prohramnoho HDL modeliuvannia dlia zakhyshchenykh informatsiinykh tekhnolohiiu [Comparison the performance of error-control code based on software HDL modeling for information security technologies]*. Infocommunication and computer technologies*, 2022).*1*(03), s.43-68.
2. Bioglio V., Condo C., Land I.) Design of Polar Codes in 5G New Radio. *IEEE Communications Surveys & Tutorials*.2020, P. 1.
3. Dumas J-G., Roch J-L., Tannier E., Varrette S. Error Detection and Correction. Foundations of Coding: Compression, Encryption, Error Correction. Wiley, 2015. pp.209-276.
4. Boiko, J., Pyatin, I., Eromenko, O., Stepanov, M). Method of the adaptive decoding of self-orthogonal codes in telecommunication. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS).* .2020. *19*(3), pp. 1287-1296.
5. Kim H. (2015). Error Correction Codes. Wireless Communications Systems Design. Wiley, P.123-207.
6. Berkman L., Turovsky O., Kyrpach L., Varfolomeeva O., Dmytrenko V., Pokotylo O. (2021). Analyzing the code structures of multidimensional signals for a continuous information transmission channel. *Eastern-European Journal of Enterprise Technologies*. *5*(9), P. 70–81.
7. Semenko A.I., Kushnir M. Ya., Bokla N. I. Sintez shirokosmugovoyi telekomunkacjnoyi sistemi z pidvishenoyu konfidencijnistyu peredachi informaciyi shlyahom vikoristannya psevdovipadkovih poslidovnostej na osnovi haosu. *Visnik universitetu «Ukrayina»*.[Synthesis of a broadband telecommunication system with increased information transmission confidentiality by using pseudo-random sequences based on chaos].. *Visnyk Visnyk universytetu «Ukrain», Seriya: informatika, obchislyuvalna tehnika ta kibernetika*. 2020. *1*(24), s.65-75 .
8. Biriukov, M., Semenko, A., Triska, NPryntsypy uzghodzhennia tsyfrovykh potokiv transportnykh telekomunikatsiinykh merezh. Принципи узгодження цифрових потоків транспортних телекомунікаційних мереж.[lignment of the transport network digital streams]. *Infocommunication and computer technologies* . 2021,. *2*(02), s. 64-80.
9. Boiko, J., Pyatin, I., Eromenko O. Pryntsypy uzghodzhennia tsyfrovykh potokiv transportnykh

telekomunikatsiinykh merezh. [Design and Evaluation of the Efficiency of Channel Coding LDPC Codes for 5G Information Technology. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*. 2021. *9*(4), pp. 867-879.
10. Boiko J., Piatin I., Karpova L., Parkhomey I. (2021). Transmission of control information in 5G broadband telecommunication systems. *Adaptivni sistemi avtomatičnogo upravlinnâ*. 2021*. 1*(38), pp. 82-95.
11. Luo F. (Deep Learning Techniques for Decoding Polar Codes. *Machine Learning for Future Wireless Communications.* 2020. pp.287-301.
12. Bae J., Abotabl A., Lin H., Song K., Lee J. An overview of channel coding for 5G NR cellular communications *APSIPA Transactions on Signal and Information Processing*. 2019. 8, E17.
13. Arikan E. Systematic Polar Coding*. IEEE Communications Letters*. *15*(8), 2011. pp. 860-862.

УДК 004.056

МЕТОДИ ПІДВИЩЕННЯ ПРИХОВАНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ

DOI 10 36994 / 2788- 5518- 2022-02-04-02

***Корчинський В.В.**, д.т.н.,проф. Державний університет інтелектуальних технологій і зв'язку, Одеса,Україна. vkadkorchin@ukr.net*

***Назаренко О.А.,** к.ф-м.н, доц. Державний університет інтелектуальних технологій і зв'язку, Одеса,Україна.* duitz.od@gmail.com

***Степанов В.О.** Військова Академія, Одеса, Україна. stepanovvadym333@gmail.com*

***Аль-Файюми Халед.** Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. khaled@alfaiomi.com*

***Анотація:** У статті розглянуто методи розширення спектра таймерних сигнальних конструкцій. Для систем радіозв'язку, що працюють в умовах радіоелектронного конфлікту, пропонується використовувати шумоподібні таймерні сигнали. Це дозволяє підвищити інформаційну, структурну та енергетичну прихованість сигнальних конструкцій. Проведено аналіз властивостей таймерних сигнальних конструкцій, що дає змогу виявити певні переваги непозиційних сигналів перед позиційними. Структурна прихованість таймерних сигналів залежить від параметрів пристрою кодування. Також таймерні сигнали можна використовувати як завадостійкий код, для якого не потрібні додаткові перевірочні елементи. За рахунок зміни параметрів побудови таймерних сигналів існує можливість змінювати коригувальну здатність коду, а також формувати різні ансамблі сигнальних конструкцій. Це потенційно збільшує структурну та інформаційну прихованість таймерних сигналів.*

Енергетична прихованість досягається за допомогою різних методів розширення спектра бінарного сигналу: псевдовипадкового перескоку робочої частоти; прямого розширення спектра псевдовипадковими послідовностями; лінійної частотної модуляції. Однак розвиток радіотехнічних засобів перехоплення широкосмугових сигналів потребує також ускладнення структури сигнальних конструкцій. Використання таймерних сигналів дає можливість синтезувати більш складні шумоподібні сигнальні конструкції. Це дозволить підвищити структурну прихованість та ускладнить розкриття структури сигналу засобами радіотехнічної розвідки супротивника. Таким чином, обґрунтованим є розробка та вдосконалення методів розширення спектра таймерних сигналів. Однак методи розширення спектра сигналів розроблялися виключно для позиційних кодів, тому не можуть бути застосовані до таймерних непозиційних сигналів. Наукові роботи, які присвячені дослідженню шумоподібних таймерних сигналів, не повною мірою висвітлюють алгоритми перетворення вузькосмугового сигналу на широкосмуговий. Це стало приводом для подальшого дослідження в цьому напрямку, тому метою цієї роботи є синтез шумоподібних таймерних сигнальних конструкцій.

***Ключові слова:** прихованість, розширення спектра, шумоподібні сигнали, захист інформації, модуляція, спектр.*

METHODS OF INCREASING SECRECY OF INFORMATION TRANSMISSION BASED ON EXPANDING THE SPECTRUM OF TIMER SIGNALS

***Vladimir Korchynskyi**, Dr. habil., Prof. State University of Intellectual Technologies and Communication, Odessa, Ukraine. vkadkorchin@ukr.net*

***Olexander Nazarenko ,** Ph.D., Ass..Prof. State University of Intellectual Technologies and Communication, Odessa, Ukraine. duitz.od@gmail.com*

***Vadim Stepanov .** Military Academy, Odessa, Ukraine. stepanovvadym333@gmail.com*

***Khaled Alfaion.** State University of Intellectual Technologies and Communications, Odessa, Ukraine. khaled@alfaiomi.com*

***Abstract:** The article considers methods of expanding the spectrum of timer signal constructions. For radio communication systems operating in conditions of electronic conflict, it is proposed to use noise-like timer signals. This will increase the information, structural and energy secrecy of signal constructions. The analysis of the properties of timer signal constructions was carried out, which made it possible to identify certain advantages of such non-positional signals over positional ones. It has been established that the information capacity of timer signals is greater than bit-digital code. The structural secrecy of timer signals depends on the parameters of the encoder. Also, such signals can be used as an error-correcting code, which doesn't require additional check elements. By changing the parameters of contracting timer signals, it is possible to change the corrective ability of the code, as well as to form different ensembles of signal constructions. This potentially increases the structural and informational secrecy of timer signals.*

Energy secrecy is achieved by using various methods of expanding the spectrum of binary signal: random jumping of the operating frequency; direct spectrum extension by random sequences; linear frequency modulation. However, the development of radio engineering means for intercepting broadband signals also requires the complication structure of signal constructions. The use of timer signals makes it possible to form more complex noise-like signal constructions. This will increase structural secrecy and complicate the disclosure of the signal structure by means of enemy electronic intelligence. Thus, it is justified to develop and improve methods for expanding the spectrum of timer signals. However, signal spreading methods were developed exclusively for positional codes, and therefore cannot be applied to non-positional timer signals. Scientific articles devoted to the research of noise-like timer signals don't fully cover the algorithms for converting narrowband signal into wideband one. This was the reason for further research in this direction, so the aim of this article is the synthesis of noise-like timer signal constructions.

Key words: secrecy, spectrum spreading, noise-like signals, information security, modulation, spectrum.

Вступ

Підвищення завадозахищеності систем радіозв'язку [1,2] є пріоритетним напрямом по захисту передаваної інформації від несанкціонованого доступу (НСД). Завадозахищеність [2] є комплексним показником, за допомогою якого оцінюється ефективність конфіденційної системи радіозв'язку. Основними показниками завадозахищеності є: завадостійкість і прихованість. Розрізняють різні види прихованості: енергетична, структурна, інформаційна, просторова та інші.

Ускладнення структури сигналу дозволяє вирішити ряд завдань по забезпеченню прихованості сигнальних конструкцій у випадку перехоплення сеансу радіозв'язку засобами радіотехнічної розвідки противника. В сучасних завадозахищених системах радіозв'язку прихованість передавання забезпечується за рахунок застосування шумоподібних сигналів [1,2]. Для цієї задачі використовуються різні методи розширення спектра сигналу: псевдовипадковий перескок робочої частоти; пряме розширення спектра за допомогою псевдовипадкових послідовностей (ППРЧ); лінійна частотна модуляція (ЛЧМ) [7]. Відомо [1,2], що теоретичною основою для формування шумоподібних сигналів є процес розширення спектра бінарної послідовності. Подальший розвиток теорії шумоподібних сигналів орієнтований на застосування таймерних сигнальних конструкцій (ТСК) [3-6], які є непозиційними. Процес формування шумоподібних ТСК потрібує іншого алгоритму, тому що існуючі методи розширення спектра здебільшого орієнтовані на позиційні сигнали. Обґрунтованість застосування шумоподібних таймерних сигналів пояснюється необхідністю ускладнення структури сигнальних конструкцій для завдання підвищення інформаційної та структурної прихованості [3-6].

Таким чином, можна відзначити, що застосування шумоподібних таймерних сигналів є пріоритетним дослідженням для завдання підвищення завадостійкості передаваної конфіденційної інформації в каналах радіозв'язку [1]. Особливість застосування таймерних сигналів полягає в тому, що вони відносяться до класу непозиційних сигнальних конструкцій та мають ряд переваг в порівнянні з позиційними, а також деякі недоліки. На основі таймерних сигналів можна реалізувати завадостійке кодування без додаткових перевірочних елементів. Зміна параметрів пристрою кодування ТСК дозволяє формувати різні ансамблі сигнальних конструкцій [8,9]. Такі властивості ТСК дозволяють вирішувати завдання по збільшенню інформаційної та структурної прихованості. Метою даної роботи є синтез шумоподібних таймерних сигнальних конструкцій на основі методів ППРЧ.

Виконання досліджень

В умовах радіоелектронного конфлікту [1,2] найчастіше в системах радіозв'язку застосовується метод розширення спектра інформаційного вузькосмугового сигналу на основі ППРЧ [2]. Пояснюється це можливістю забезпечення для передаваного сигналу певної енергетичної прихованості, яка досягається за рахунок зміни частоти носійного коливання для одного або кількох біт у заданому достатньо великому діапазоні частот. Закон зміни передаваної частоти носійного коливання відомий тільки передавачеві та приймачеві, та може змінюватися від одного сеансу передачі до іншого. Перехоплення такого сигналу без знання цього закону зміни частот може бути лише за допомогою широкодіапазонного сканера приймача противника, що не завжди може бути успішним при великій кількості працюючих радіостанцій з ППРЧ. Існує кілька варіантів розширення спектра за допомогою ППРЧ. В залежності від кількості біт, що передаються на одній частоті розрізняють швидку і повільну ППРЧ [2].

При швидкій ППРЧ тривалість передавання одного інформаційного елемента t_0 розрядно-цифрового коду на одній частоті може бути:

$$t_{\text{пер}} \le t_0. \quad (1)$$

При повільній ппрч на одній частоті $\Delta f_{\text{прч}}$ передається кілька біт, тобто:

$$t_{\text{пер}} > t_0. \quad (2)$$

Розглянемо можливість розширення спектра таймерного сигналу [3] з урахуванням особливостей його побудови. Таймерний сигнал є непозиційним, і базовим часовим елементом для його побудови є інтервал часу Δ. Далі задається інтервал побудови ТСК:

$$T_c = nt_0, \quad (3)$$

де n – кількість елементів Найквиста t_0.

В часових границях сигнальної конструкції T_c тривалість імпульсів :

$$t_c = t_0 + \Delta \times l, \quad (4)$$

де $l \in 0, 1, 2, 3, \ldots$ і кратне $\Delta = t_0/s$ ($s \in 2, 3, \ldots k$).

Відстань між значущими моментами модуляції (ЗММ) ($t_c \ge t_0$) не менша за інтервал Найквіста ($t_0 = 1/\Delta F_c$) і кратна елементу Δ. Така умова дозволяє усунути міжсимвольні спотворення в ТСК. Число s показує, наскільки менше часовий інтервал Δ по відношенню до t_0. Число переходів i в ТСК може бути різним і змінюватися в межах $i = 1, 2, ..., n-1$.

На рис. 1 (а) надана часова діаграма реалізації ТСК на інтервалі $T_c = 4t_0$.

Як бачимо, тривалість імпульсу ТСК t_c може бути більше t_0, тому застосувати умову (1) або (2) для розширення спектра таймерних сигналів за допомогою швидкої або повільної ППРЧ не є можливим. Тобто, основною проблемою для цього є непозиційність ЗММ в ТСК по відношенню до інтервалу Найквиста t_0.

Розширення спектра ТСК за допомогою методу швидкої ППРЧ

Розглянемо випадок, коли тривалість передавання на частоті носійного коливання $t_{\text{пер}} < t_0$ та $t_{\text{пер}} \le \Delta$. Це дає можливість реалізувати швидку ППРЧ, використовуючи інтервал Δ для передачі однієї або кількох частот. Для реалізації цього методу запропоновано спочатку виконати пряме розширення спектра ТСК за допомогою псевдовипадкової послідовності $c(T_c)$ (рис. 1 б) з тривалістю імпульсу τ.

Спектр ТСК $x_{\text{тск}}(t_c)$ розширюється за допомогою елементів :

$$\tau = \Delta / j \quad (5)$$

де j =1, 2, 3, … – кількість елементів τ на інтервалі Δ.

Перетворення ТСК за допомогою псевдовипадкової послідовності $c(T_c)$ (рис. 1 (б)) в широкосмуговий сигнал (рис. 1 (в)) відбувається за наступною формулою:

$$x_{\text{скк}}(T_c) = x_{\text{тск}}(t_c) \times c(T_c). \quad (6)$$

Далі відбувається розширення спектра вже широкосмугового ТСК $x_{\text{скк}}(T_c)$ за допомогою швидкої ППРЧ (рис. 1 (г)):

$$u'(t) = x_{\text{скк}}(T_c) U_0 \cos(\omega(g(t)t)), \tag{7}$$

де $\cos(\omega(g(t)t))$ – набір частот, який являє собою функцію від кодового сигналу $g(t)$.

Розширення спектра ТСК за допомогою методу повільної ППРЧ

Для методу повільної ППРЧ при розширенні спектра бітів розрядно-цифрового коду швидкість зміни частоти носійного коливання більше в кілька разів інтервалу Найквіста t_0. В таймерних сигналах $\Delta < t_0$, тому час зміни частоти носійного коливання $T_{\text{М ППРЧ}}$ для повільної ППРЧ буде визначатися з урахуванням елемента Δ, тобто:

$$T_{\text{М ППРЧ}} = \Delta z, \tag{8}$$

де $z = 2, 3, \ldots, M$ – кількість елементів Δ на інтервалі $T_{\text{М ППРЧ}}$; $M = ns$.

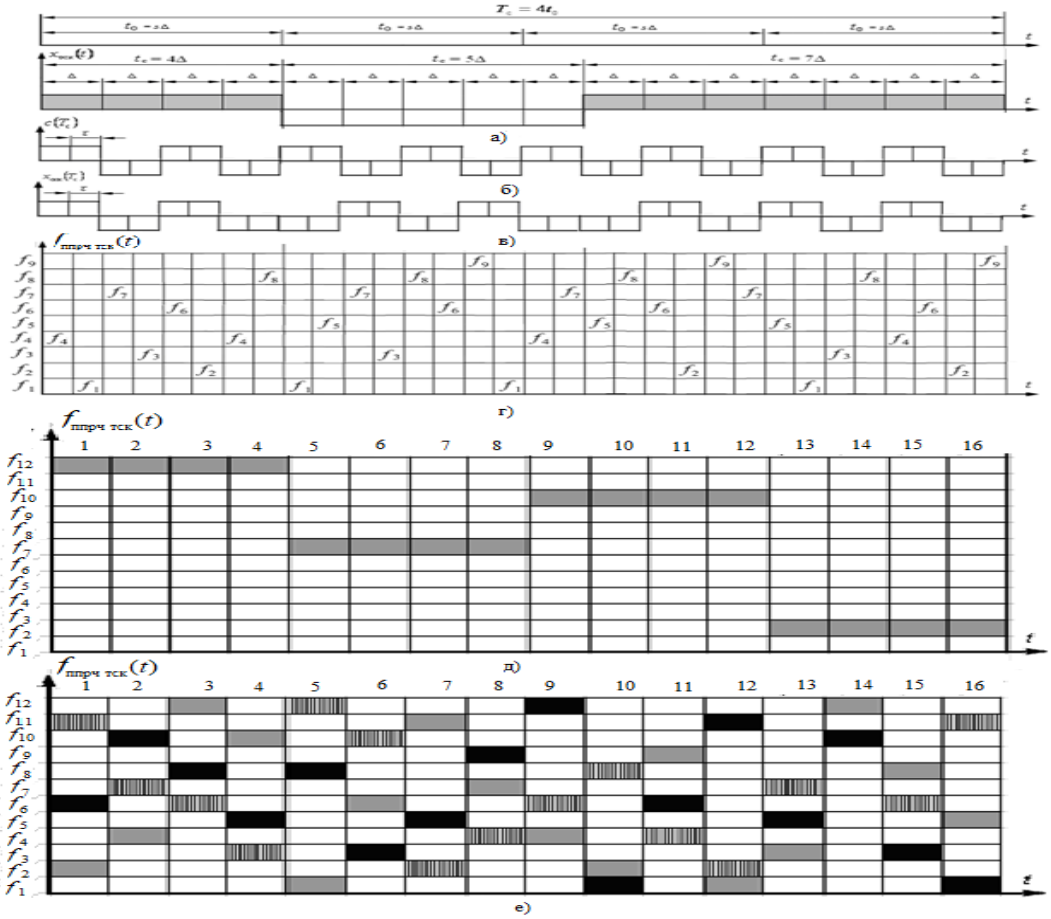


Рис 1. Розширення спектра ТСК $x_{\text{тск}}(t_c)$ за допомогою ПВП (в), методами швидкої (г) та повільної (д) ППРЧ, багатоканальної ППРЧ (е) на інтервалі $T_c = 4t_0$

При виборі часового інтервалу зміни частоти носійного коливання слід брати до уваги, що при збільшенні значення $T_{\text{М ППРЧ}}$ ймовірність ураження завадою сигналу в радіоканалі підвищується. На рис. 2 (д) надано процес розширення спектра методом повільної ППРЧ з

інтервалом $T_{\text{М ППРЧ}} = 4\Delta$, де $z = 4$. Якщо $z = M$, тоді зміна частоти носійного коливання відбуватиметься на інтервалі:

$$T_{\text{М ППРЧ}} = T_{\text{с}}, \tag{9}$$

тобто для кожної сигнальної конструкції. За умови (9) кожна таймерна сигнальна конструкція передається на певній частоті носійного коливання.

Вочевидь, що для визначення значущих моментів відновлення (ЗМВ) фронтів ТСК [3]на приймальній стороні необхідно в передавачі після прямого розширення спектра використовувати попередню маніпуляцію елементів Δ або τ (за умови, що $\tau \neq \Delta$), наприклад, ФМ-2, ФМ-4 або КАМ-4. Так при ФМ-4 або КАМ-4 (квадратурна-амплітудна модуляція) можна забезпечити збільшення швидкості передавання інформації за рахунок того, що на одну сигнальну конструкцію аналогового сигналу передаються два елементи Δ в порівнянні з ФМ-2. Застосування більш складних видів модуляції для підвищення швидкості передавання інформації, наприклад, КАМ-8 або КАМ-16, призведе до зниження завадостійкості системи радіозв'язку.

Для методу швидкої ППРЧ (рис. 2 (в)) часовий інтервал несучої частоти $T_{\text{Б ППРЧ}}$ збігається або менше елемента Δ:

$$T_{\text{Б ППРЧ}} \leq \Delta. \tag{10}$$

Слід зазначити, що метод швидкої ППРЧ більш стійкий до завад. У разі впливу вузькосмугової завади, яка спотворює сигнал в певному підканалі, не відбувається повного спотворення сигнальної конструкції, так як рівень імпульсу в межах $t_{\text{с}} = t_0 + k\Delta$ повторюється по Δ кілька разів на різних частотних підканалах. Як правило, таке спотворення призводить до дроблення одного або декількох імпульсів ТСК, що виявляється приймачем при демодуляції.

При повільній ППРЧ вплив вузькосмугової завади може привести до суттєвого спотворення структури таймерного сигналу, що ускладнює процес його відновлення на приймальній стороні. Однак цей метод простіший в реалізації, ніж метод швидкої ППРЧ.

Розширення спектра ТСК за допомогою методу багатоканальної швидкої ППРЧ

На рис. 1 (е) надано метод багатоканальної швидкої ППРЧ на основі ТСК. За рахунок передавання одного елемента Δ на різних частотах носійного коливання f_i цей метод дозволяє підвищити стійкість системи радіозв'язку до завад. Використання непарного числа підканалів f_i, наприклад, w = 3 (рис. 1 г), дозволить реалізувати оцінку якості прийнятого елемента Δ за мажоритарним принципом, що суттєво підвищить завадостійкість системи радіозв'язку. При цьому остаточне рішення про стан прийнятої ТСК буде здійснюватися шляхом визначення приналежності її до підмножини дозволених та недозволених сигнальних конструкцій.

На рис. 2 надано структурну схему завадозахищеної системи зв'язку з шумоподібними таймерними сигналами. Джерело повідомлення (ДП) видає на пристрій завадостійкого кодування (ПЗК) розрядно-цифрового коду інформаційну двійкову послідовність k. ПЗК виконує завадостійке кодування та добавляє до інформаційної послідовності перевірочні символи r, тобто загальна довжина комбінації [3]:

$$n = k + r. \tag{11}$$

З виходу ПЗК елементи РЦК поступають на кодер таймерних сигналів (КДТСК). Сформовані ТСК з виходу КДТСК подаються на помножувач, де відбувається розширення спектра таймерних сигналів за допомогою псевдовипадкових послідовностей, наприклад Уолша. Далі в пристрої $М_{ФМ}$ відбувається фазова маніпуляція елементів розширеної послідовності. Помножувач ☒ за допомогою частот носійного коливання, що формуються синтезатором робочих частот, переносяться в спектр високих частот.

Таким чином, процес розширення спектра відбувається за рахунок двох методів: прямого розширення спектра та швидкої ППРЧ. Генератор ключів служить для формування параметрів

таймерних сигналів та закону генерування псевдовипадкових послідовностей синтезатора робочих частот. Робота генератора ключів відбувається за допомогою вхідних параметрів.

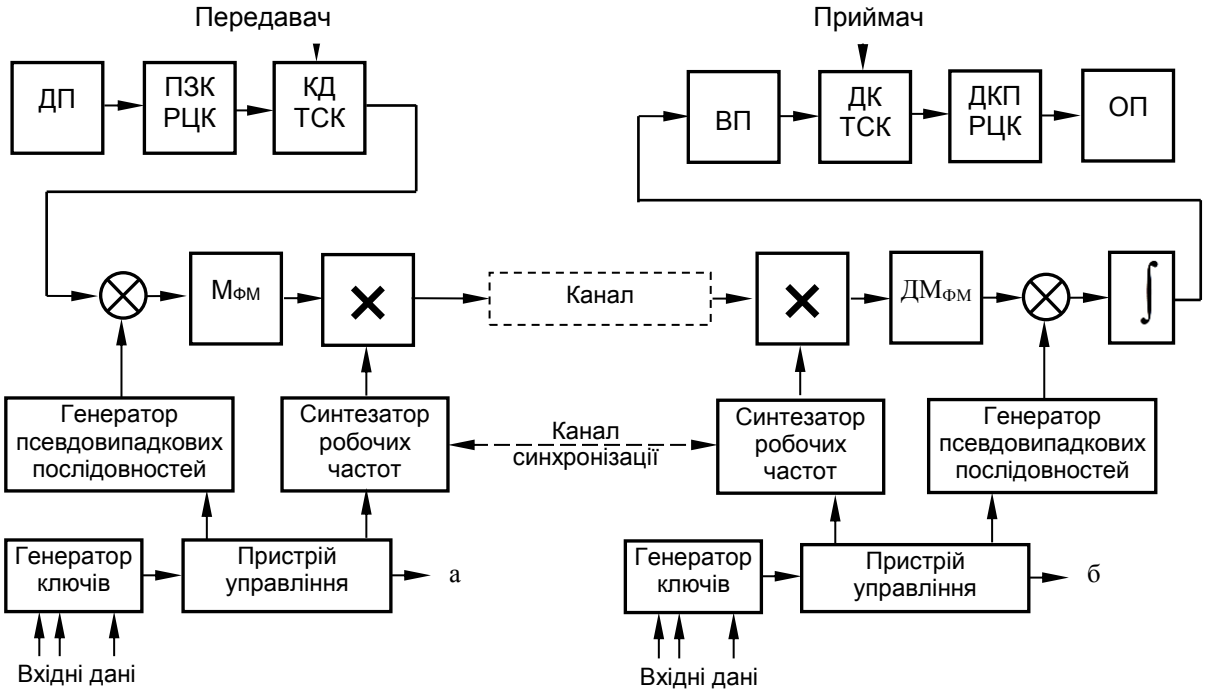


Рис. 2. Структурна схема завадозахищеної системи зв'язку з ТСК та ППРЧ: ДП – джерело повідомлення; ПЗК – пристрій завадостійкого кодування РЦК; КД – пристрій кодування ТСК; Мфм – фазовий маніпулятор; ДМфм – демодулятор фазових сигналів; ⊠ – помножувач; ∫ – інтегратор; ВП – вирішальний пристрій

Висновки

1. Запропонований метод формування шумоподібних сигналів на основі непозиційних таймерних сигнальних конструкцій вимагає застосування двох етапів розширення спектра, що дозволяє вирішити ряд завдань з підвищення прихованості та завадостійкості.

2. На першому етапі пропонується пряме розширення спектра ТСК з маніпуляцією елементів псевдовипадкової послідовності, що підвищує структурну прихованість сигнальних конструкцій, а також вирішує проблему визначення ЗМВ в приймачі.

3. На другому етапі використовується один із розглянутих методів ППРЧ, при цьому перенос спектра в область високих частот відбувається для одного або кількох елементів розширення псевдовипадкової послідовності. Також можливий варіант застосування швидкої ППРЧ за умови, коли тривалість передавання частоти носійного коливання менше за елемент розширення псевдовипадкової послідовності.

4. Застосування двох етапів розширення спектра ТСК потребує ускладнення системи радіозв'язку, в якій потрібно застосовувати додаткові пристрої: в передатчику – це пристрій прямого розширення спектра, а в приймачі – пристрій кореляційного прийому.

Література

1. Куприянов А.И.,Захаров А.В. Теоретические основы радиоэлектронной борьбы. М.: Вузовская книга, 2007. 356 с.

2.Борисов. В.И., Зинчук В.М., Лимарев А.Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты , под ред. Борисова В.М.. М.: Радио и связь, 2000. 384 с.

3. Захарченко В.М. Синтез багатопозиційних часових кодів. Київ: Техніка, 2012. 284 с.

4. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012) – Lviv; Publishing House of Lviv Polyteshnic, 2012. C. 317.

5. Zakharchenko M. Integrated methods of information security in telecommunication systems / Zakharchenko M.,

Korchynskii V., Kildishev V. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.

6. Skopa O. Korchinsky. V. Management of Relative Effective Transmission Rate in Packet Switching Networks . Proceedings of the International Conference TCSET'2002, February 18-23, 2002 Lviv-Slavsko, Ukraine, 2 p.

7. Volodymyr Korchinskyi, Matin Hadzhyiev, Pavlo Pozdniakov, Vitalii Kildishev, Valeriy Hordiichuk Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals . *Eastern-European Journal of Enterprise Technologies / Information and controlling system.*2018. №6/9(96). Vol 6.pp.. 29-37.

8. Korchynskyi V. V., Kildishev V. I., Holev D.V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding // National University «Zaporizhzhia Polytechnic» Radio Electronics, Computer Science, Control The scientific journal, 2019. № 3(50). pp. 108-116.

9. V Hordiichuk, A Shyshatskyi2, V Korchinskyi, Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems 1*, Journal of Physics: Conference Series* .2021. ICOLSSTEM 2020 IOP Publishing.

References

1. Kupriyanov A.I. , Sakharov A. V. Teoreticheskie osnovy radio`elektronnoj bor'by.[Theoretical foundations of electronic warfare]. M.: University book, 2007. 356 p.

2. Borisov V.I. Zinchuk V.M., Limarev A.E. Pomehozaschischennost' sistem radiosvyazi s rasshireniem spektra signalov metodom psevdosluchajnoj perestrojki rabochej chastoty , pod red. Borisova V.M.[Noise Immunity of Radio Communication Systems with Signal Spectrum Spreading by the Method of Pseudo-Random Frequency Tuning]. M.: Radio i svyaz', 2000. 384 p.

3. Zakharchenko V.M. Sintez bagatopozicijnih chasovih kodiv. [Synthesis of rich positional clock codes] Kyiv: Technique, 2012. 284 p.

4. Zakharchenko N. Information security of Time-Controlled Signals in Confidential Communication Systems / N. Zakharchenko, V. Korchinsky, B. Radzimovsky // Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 february 2012) – Lviv; Publishing House of Lviv Polyteshnic, 2012. C. 317.

5. Zakharchenko M. Integrated methods of information security in telecommunication systems / Zakharchenko M., Korchynskii V., Kildishev V. 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library. 11 – 15 September 2017. – V. 1. – pp. 78–81. URL: http://ieeexplore.ieee.org/document/8095366/.

6. Skopa O. Korchinsky. V. Management of Relative Effective Transmission Rate in Packet Switching Networks . Proceedings of the International Conference TCSET'2002, February 18-23, 2002 Lviv-Slavsko, Ukraine, 2 p.

7. Volodymyr Korchinskyi, Matin Hadzhyiev, Pavlo Pozdniakov, Vitalii Kildishev, Valeriy Hordiichuk Development of the procedure for forming non-stationary signal structures based on multicomponent LFM signals . *Eastern-European Journal of Enterprise Technologies / Information and controlling system.*2018. №6/9(96). Vol 6.pp.. 29-37.

8. Korchynskyi V. V., Kildishev V. I., Holev D.V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding // National University «Zaporizhzhia Polytechnic» Radio Electronics, Computer Science, Control The scientific journal, 2019. № 3(50). pp. 108-116.

9. V Hordiichuk, A Shyshatskyi2, V Korchinskyi, Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems 1*, Journal of Physics: Conference Series* .2021. ICOLSSTEM 2020 IOP Publishing.

УДК 520.272.2: 621.396.677.494

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ СИСТЕМИ ЧАСУ ТА ЧАСТОТИ РНДБ РАДІОТЕЛЕСКОПА В НАЦІОНАЛЬНУ СЛУЖБУ ЄДИНОГО ЧАСУ ТА ЕТАЛОННИХ ЧАСТОТ

DOI 10 36994 / 2788- 5518- 2022-02-04-03

Гайдаманчук В.А., *к.т.н. WIRCOM, Київ, Україна. gva@wircom.ua*
Матвієнко М.В. *WIRCOM, Київ, Україна. mnv@wircom.ua*
Пастушенко І.М. *WIRCOM, Київ, Україна. inp@wircom.ua*

Анотація: *Статтю присвячено особливостям модернізації Національної служби єдиного часу та еталонних частот (НСЄЧЕЧ) для підвищення її надійності та доступності для користувачів за рахунок включення в її склад системи часу та частоти, яка розроблена для забезпечення потреб РНДБ (Радіоінтерферометрія з НадДовгою Базою) радіотелескопа. В роботі подано характеристики, які повинна забезпечувати система частоти та часу РНДБ радіотелескопа. Розглянуто основні принципи побудови системи частоти та часу РНДБ радіотелескопа RT-32 на базі антенної системи MARK-4B та технічні передумови для її інтеграції в НСЄЧЕЧ. Наведені приклади технічних рішень з побудови системи частоти та часу РНДБ радіотелескопа, можливостей обміну сигналами точного часу по оптичній мережі загального користування між такою системою та еталонами частоти та часу, які входять до складу НСЄЧЕЧ.*

Ключові слова: *радіотелескоп, синхронізація часу, синхронізація частоти, служба єдиного часу та еталонних частот, мазер, РНДБ, RT-32, VLBI, EVN, BIPM, GPS, GNSS, PTP, PTSS, UTC, ITU.*

FEATURES OF THE VLBI RADIO TELESCOPE PRECISE TIME SCALE SYSTEM INTEGRATION INTO THE NATIONAL TIME SYNCHRONIZATION AND REFERENCE FREQUENCIES SERVICE

Viktor Gaidamanchuk, *Ph.D.WIRCOM, Kyiv, Ukraine. gva@wircom.ua*
Mykola Matvienko. *WIRCOM, Kyiv, Ukraine. mnv@wircom.ua*
Ihor Pastushenko. *WIRCOM, Kyiv, Ukraine. inp@wircom.ua*

Abstract: *The article is devoted to the problems of the possibility of expanding the time synchronization and reference frequencies service by including in its composition a time and frequency system designed to meet the needs of the VLBI radio telescope. The paper presents the characteristics provided by the frequency and time system of the VLBI (Very Long Baseline Interferometry) radio telescope. The basic principles of building the frequency and time system of the VLBI radio telescope and the technical prerequisites for its integration into the time synchronization and reference frequencies service were considered. Examples of technical solutions for building frequency and time system for VLBI radio telescope RT-32 Zolochiv and delivering accurate time signals to remote users based on modern ITU-T and IEEE recommendations are given. These technical solutions can be successfully taken into account during the development and modernization of the time synchronization and reference frequencies service. The main factors that ensure the compatibility of the time and frequency system of the VLBI radio telescope and time synchronization and reference frequencies service are considered. The need to improve the frequency and time system of the VLBI radio telescope by means of the addition of atomic standards and the use of system solutions for the organization of the group time scale is substantiated, which makes it possible to achieve the level of characteristics that provide both the requirements for the frequency and time stability of radio telescopes of the European VLBI Network (EVN) level and allow to integrate into the National time synchronization and reference frequencies service. The results of the research also demonstrate the possibility of integrating the frequency and time systems of the VLBI radio telescope and National time synchronization and reference frequencies service using PTP IEEE 1588-2008 protocol (Profile PTP unicast ITU-T G.8275.2) and the DWDM public optical network «Eurotranstelecom» (Ukraine) for their connection at distances up to 760 km.*

Key words: *radio telescope, timing, time synchronization and reference frequencies service, time scale system, maser, VLBI, RT-32, EVN, BIPM, GPS, GNSS, PTP, PTSS, UTC, ITU.*

Вступ

Поряд з підвищенням вимог до точності часу підвищуються також вимоги до надійності забезпечення сигналами синхронізації часу в різних галузях критичної інфраструктури. Як відомо, найбільш розповсюдженим та доступним джерелом сигналів синхронізації точного часу є сигнали GPS, але вони, як і сигнали інших систем GNSS, вразливі до різноманітних перешкод, що не забезпечує високої надійності доставки сигналів синхронізації точного часу до критично чутливих до точності споживачів. Крім того, вони вразливі також до природних дестабілізуючих факторів, таких як влучання блискавки, обмерзання антен, сонячні спалахи, атмосферні явища. Загрозу для систем GNSS становлять також навмисні перешкоди, які можуть спеціально застосовуватися зловмисниками.

Асоціація телекомунікаційних організацій США (ATIS) для збільшення надійності систем синхронізації часу рекомендує використовувати в якості резервних сигнали від альтернативних до GNSS джерел часу відповідної якості [1]. Одним із вирішень проблеми є використання сигналів точного часу Національної служби єдиного часу і еталонних частот (НСЄЧЕЧ) [2]. Для цього мережа, по якій необхідно доставити сигнал синхронізації часу до серверів часу з мінімальною похибкою, повинна охоплювати велику площу і затримка сигналу по лінії зв’язку (оптичному волокну) має бути мінімальною, а тому є доцільним прагнути до побудови НСЄЧЕЧ на основі ансамблю еталонів з їх оптимальним наближенням до споживачів сигналів в регіонах. При цьому дуже важливим стає або створення додаткових еталонів для досягнення цієї мети або інтеграція в НСЄЧЕЧ вже наявних в країні технічних рішень, якщо їх рівень характеристик відповідає вимогам до еталонів, з яких складається НСЄЧЕЧ.

Безумовно, до одних з найбільш відповідних для досягнення такої мети технічних рішень належать системи частоти та часу, які застосовуються в РНДБ радіотелескопах. Тому у разі наявності в країні РНДБ радіотелескопів є раціональним розглядати їх системи частоти та часу як наявний резерв для інтеграції в НСЄЧЕЧ з метою підвищення як її надійності, так і регіональної доступності її сервісів, зважаючи на певні мережеві обмеження доставки прецизійних сигналів часу споживачам.

Виконання досліджень

На рис. 1 представлені характеристики атомних стандартів частоти, на основі яких працюють системи частоти та часу радіотелескопів РНДБ [3] і які також входять як еталони до складу НСЄЧЕЧ. Системи частоти та часу РНДБ радіотелескопів, а також первинні та вторинні еталони частоти та часу НСЄЧЕЧ базуються на формуванні автономної атомної групової шкали часу з використанням атомних (Maser, Cs) стандартів частоти з можливістю звірення цієї шкали з Національною шкалою часу або шкалою часу UTC з високою точністю. Відомим технічним рішенням побудови таких систем є розробка компанії Symmetricom – Precise Time Scale System (PTSS) [4].

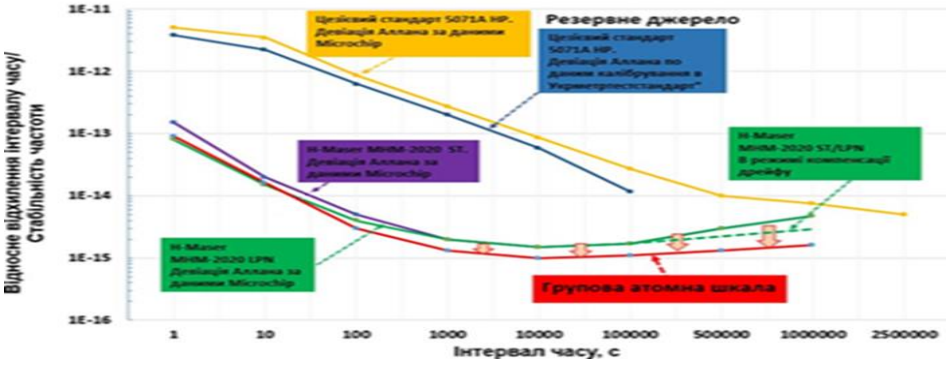


Рис.1. Характеристики атомних стандартів та групової атомної шкали часу системи частоти та часу РНДБ радіотелескопа після її удосконалення

Це повноцінний апаратно-програмний комплекс з можливістю формування автономної атомної шкали часу на базі атомних стандартів частоти (Maser, Cs), функцією звірення цієї шкали з шкалами часу UTC з високою точністю та базою даних розходження цих шкал. Враховуючи це, система частоти та часу РНДБ радіотелескопа при застосуванні відповідного рівня обладнання технічно може забезпечити рівень параметрів, який задовольнить вимогам НСЄЧЕЧ [5]. Структурна схема базового технічного рішення такої системи частоти та часу РНДБ радіотелескопа RT-32 [6,7], реалізованого на основі обладнання Microchip, представлена на рис. 2. Зовнішній вигляд стенда з обладнанням, яке входить до складу системи частоти та часу РНДБ радіотелескопа RT-32 – на рис. 3.

Результати визначення похибки вимірювання розходження автономної шкали часу (на основі цезієвого стандарту 5071A) та шкали часу UTC, сформованої PTP сервером TimeProvider 4100 (вихід 1PPS) протягом 11-ти діб в процесі дослідної експлуатації (СКВ похибки, не більше 8,48 нс) подані на рис. 4.

В подальшому така система часу та частоти може бути вдосконалена за рахунок додавання атомних стандартів та використання групової шкали часу (рис. 5, 6), що дозволить при такій реалізації досягнути рівня характеристики «Групова атомна шкала», поданої на рис. 1, і ефективно забезпечувати як вимоги до стабільності частоти та часу сучасних мереж РНДБ радіотелескопів, таких як EVN (European VLBI Network), так і вимоги до Національних еталонів частоти та часу відповідно до вимог BIPM [8].

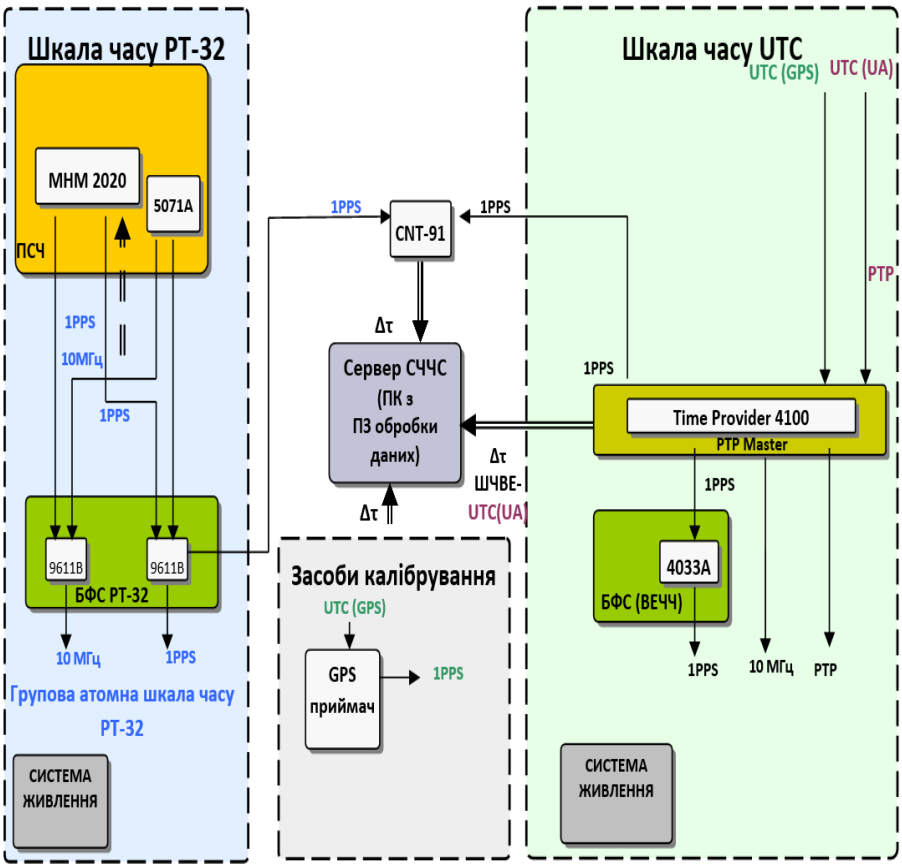


Рис. 2. Структурна схема системи частоти та часу РНДБ радіотелескопа RT-32

Рис. 3. Зовнішній вигляд системи частоти та часу РНДБ радіотелескопа RT-32 Золочів

Важливим технічним завданням, яке необхідно вирішити для реалізації інтеграції системи частоти та часу РНДБ радіотелескопа в НСЄЧЕЧ, є її під’єднання за допомогою оптичних чи супутникових технологій до одного з Національних еталонів для проведення періодичних сеансів звірення їх шкал часу [9].

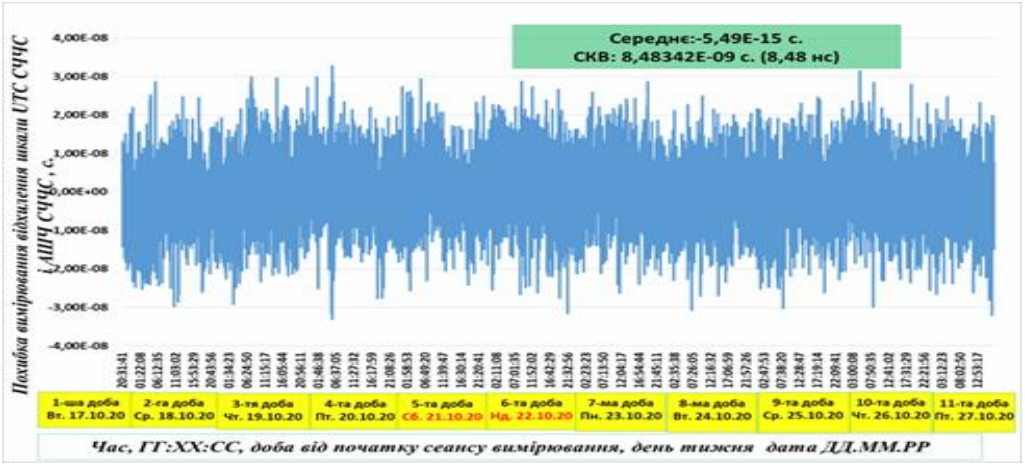


Рис. 4. Похибка вимірювання розходження автономної шкали часу та шкали часу UTC в процесі дослідної експлуатації системи часу та частоти РНДБ радіотелескопа RT-32 Золочів

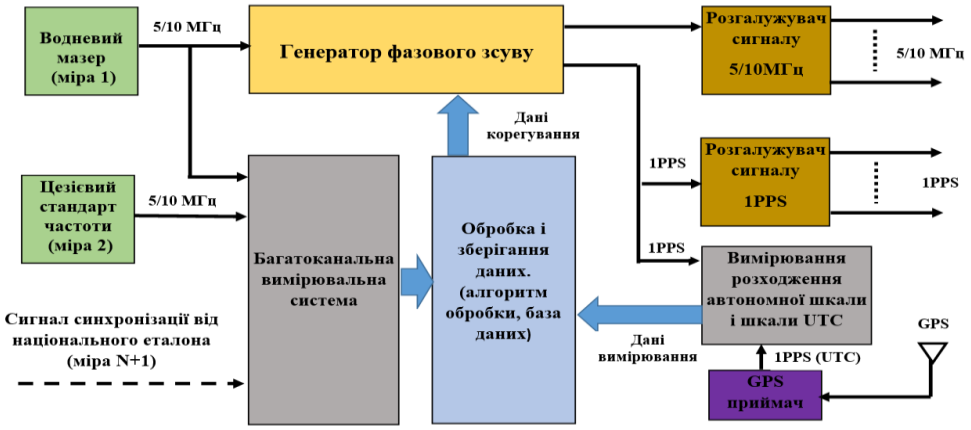


Рис. 5. Структурна схема формування групової атомної шкали часу РНДБ радіотелескопа

При цьому для забезпечення відповідної нормативам НСЄЧЕЧ якості передачі міток часу по пакетній мережі слід враховувати можливі складові похибки, які виникають при проходженні пакетів по мережі, – постійну складову похибки, яка виникає за рахунок наявності мережевої асиметрії та затримки буферизації пакетів, і динамічну складову похибки. Також треба враховувати, що при використанні протоколу PTP IEEE 1588–2008 асиметрія затримки пакетів виникає й внаслідок зміни швидкості інтерфейсу елементів мережі PTP.

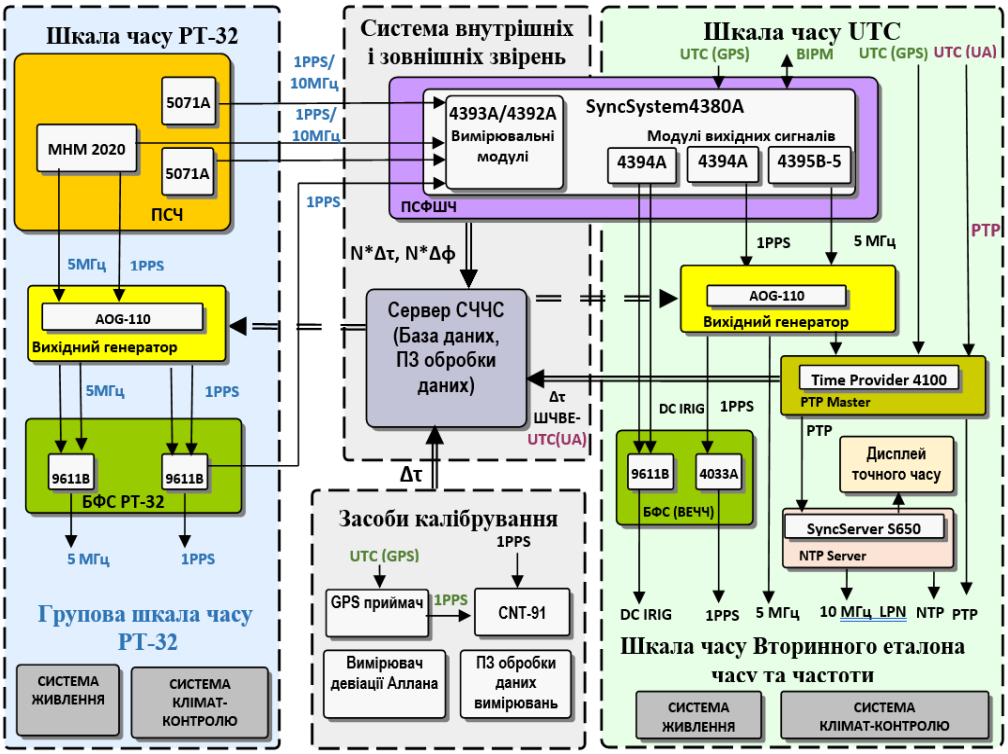


Рис.6. Структурна схема системи частоти та часу РНДБ радіотелескопа з використанням групової атомної шкали часу

Інтеграція систем часу та частоти РНДБ радіотелескопів в НСЭЧЕЧ активно впроваджується в різних країнах ЄС [10]. Передача еталонних сигналів часу та частоти від РНДБ радіотелескопів до національних еталонів часу та частоти і в зворотному напрямку може здійснюватись по оптичній лінії зв'язку різними методами (одно- або двосторонньою передачею опорних сигналів частоти несучої або модульованої, за протоколом PTP з процедурою калібрування та компенсації асиметрії). Для зв'язку між РНДБ радіотелескопами та національними еталонами використовуються «темне» оптичне волокно та DWDM канал.

В рекомендаціях ITU-T G.8271 [11] передбачені засоби для компенсації асиметрії, яка виникла за рахунок буферизації кадрів. Очікувану асиметрію можна оцінити, спираючись на розмір пакета повідомлень PTP та швидкість інтерфейсів.

Таку асиметрію може бути компенсовано за допомогою механізму компенсації асиметрії (розділ 11.6 IEEE 1588-2), алгоритм якого використовують сучасні сервери часу, наприклад, TimeProvider 4100, який був використаний в ході досліджень.

Причинами виникнення асиметрії, наприклад, при застосуванні оптичних мереж також є:

- використання різних довжин хвиль в прямому та зворотному напрямках при застосуванні технології DWDM в оптичній мережі;
- передача сигналів синхронізації різними волокнами;

різний показник заломлення волокон. Проведені тестування якості передачі міток .часу на загальну відстань 760 км (рис. 7) з використанням технологій DWDM та APTS дозволяють на основі отриманих результатів стверджувати про можливість забезпечити передачу міток часу на рівні, що відповідає вимогам до НСЄЧЕЧ. Для тестування було використано обладнання Microchip TimeProvider 4100 Software Version 1.0.5 з використанням Profile PTP unicast ITU-T

G.8275.2 мережевого протоколу синхронізації часу PTP IEEE 1588-2008 з налаштуваннями: (one-step, Sync–64/s, Delay-reg–64/s, Announce–4/s). Один з з двох TimeProvider 4100 використовувався як «*Grandmaster PTP*», а інший як «*Client PTP*». Контроль точності синхронізації часу здійснювався за допомогою вбудованої функції TimeProvider 4100 – моніторингу точності синхронізації часу. Пакетне навантаження Ethernet мережі при тестуванні не перевищувало 20%.

Відповідно до висунутих вимог з точності синхронізації часу при модернізації національної мережі єдиного часу необхідно врахувати вище наведені причини виникнення похибки часу та в разі необхідності застосовувати технології компенсації асиметрії (APTS) та різноманітні режими, передбачені протоколами PTP IEEE 1588-2008 [12].

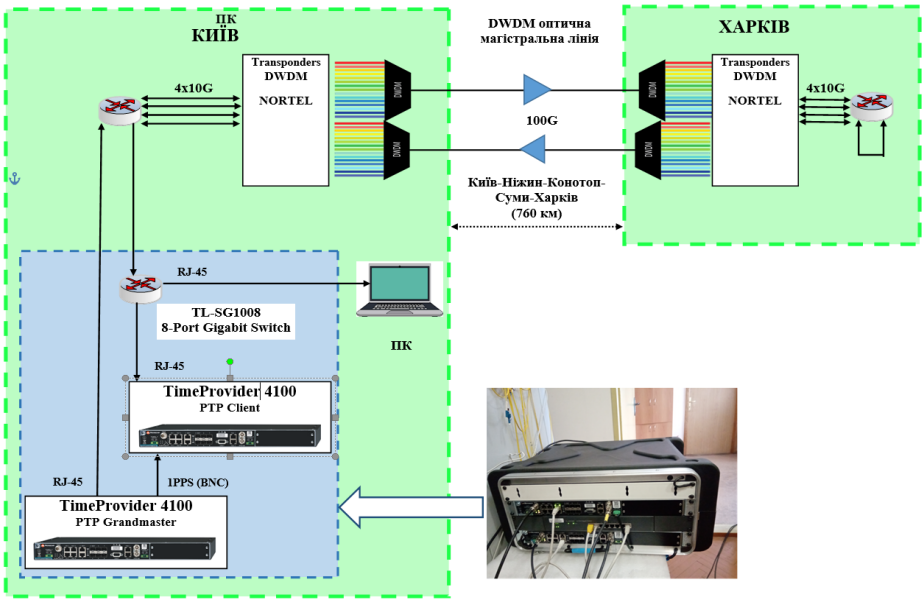


Рис.7.Схема вимірювання похибки синхронізації часу при використанні протоколу PTP 1588 на магістральній оптичній мережі DWDM «Євротранстелеком»

Проведені тестування якості передачі міток часу на загальну відстань 760 км (див.рис. 7) з використанням технологій DWDM та APTS дозволяють на основі отриманих результатів стверджувати про можливість забезпечити передачу міток часу на рівні, що відповідає вимогам до НСЄЧЕЧ. Для тестування було використано обладнання Microchip TimeProvider 4100 Software Version 1.0.5 з використанням Profile PTP unicast ITU-T G.8275.2 мережевого протоколу синхронізації часу PTP IEEE 1588-2008 з налаштуваннями: (one-step, Sync–64/s, Delay-reg–64/s, Announce–4/s). Один з з двох TimeProvider 4100 використовувався як «*Grandmaster PTP*», а інший як «*Client PTP*». Контроль точності синхронізації часу здійснювався за допомогою вбудованої функції TimeProvider 4100 – моніторингу точності синхронізації часу. Пакетне навантаження Ethernet мережі при тестуванні не перевищувало 20%.

Висновки

Розглянуті особливості інтеграції систем часу та частоти РНДБ радіотелескопів в НСЄЧЕЧ та проведені дослідження дозволяють стверджувати, що технічний рівень систем часу та частоти РНДБ радіотелескопів, сучасних оптичних мережевих технологій та досягнення в реалізації використання синхронізації часу відповідно до вимог протоколу PTP 1588 можуть ефективно розширити можливості НСЄЧЕЧ, особливо за рахунок резервування та покращення регіональної розгалуженості та наближення до користувачів.

Наведені результати демонструють, як за допомогою протоколу PTP 1588 та оптичної мережі загального користування можна реалізувати інтеграцію системи частоти та часу РНДБ радіотелескопа та створити мережу синхронізації часу відповідно до вимог НСЄЧЕЧ.

Треба зазначити, що в процесі досліджень при забезпеченні вказаних умов та при використанні опцій High-Performance Boundary Clock та Enhanced Primary Reference Time Clocks, які доступні в сучасних серверах часу, похибка часу не перебільшувала 10 нс.

Розширення НСЄЧЕЧ за рахунок інтеграції в неї системи частоти та часу радіотелескопа РНДБ, використовуючи при цьому вже існуючу національну мережеву інфраструктуру на основі оптичних ліній зв'язку дозволить:

- забезпечити доступ критичних до точності часу галузей України, в тому числі оборонного призначення, до надійних сигналів точного часу НСЄЧЕЧ;
- підвищити надійність та точність як системи частоти та часу РНДБ радіотелескопа, так і еталонів НСЄЧЕЧ;
- в перспективі забезпечить можливість приєднання НСЄЧЕЧ до міждержавних мереж синхронізації часу і частоти.

Література

1. ATIS-0900005. GPS Vulnerability. Technical Report. Alliance for Telecommunications Industry Solutions. Approved September 7, 2017. 23 p.
2. Постанова Кабінету Міністрів України від 2 вересня 2015 р. № 664 "Питання Служби єдиного часу і еталонних частот". URL: https://zakon.rada.gov.ua › 664-2015-п
3. Istituto Nazionale di Ricerca Metrologica (INRIM) Report to the 20th Meeting of the CCTF INRIM's Time and Frequency Activities. September 2015. 16 p.
4. Symmetricom Datasheet «Precise Time Scale System». URL: https://www.microsemi.com/product-directory/time-frequency-systems/4156-precise-time-scale-system#resources
5. Michael A. Lombardi et. al. Accurate, Traceable, and Verifiable Time Synchronization for World Financial Markets. *Journal of Research of the National Institute of Standards and Technology.* Volume 121, 2016. pp. 436-463.
6. Ульянов О., Чмиль В., Яцкив Я. и др. Создание радиотелескопа РТ-32 на базе антенной системы MARK-4B. 1. Проект модернизации и первые результаты. *Радіофізика і радіоастрономія.* 2019. Т. 24. № 2. С. 87–116.
7. Viktor Gaidamanchuk. Results of development VLBI time scale system RT-32 Zolochiv. *International Workshop "RT-32 Zolochiv: First Results, EU Collaboration, Radio Astronomy Frontiers".* Zolochiv, Ukraine, 3-5 October 2021. URL: https://spacecenter.gov.ua/contents/uploads/2021/10/Viktor-Gaidamanchuk__Results-of-Develompent-VLBI-Time-Scale-System-RT-32-Zolochiv.pdf
8. Gerard Petit Atomic time scales TAI and TT (BIPM): Present status and prospects. *Proceedings of the 7th Symposium Frequency Standards and Metrology*. 2009. pp. 475–482.
9. Ł. Śliwczyński et. al. Remote synchronization of atomic clocks. 2016 21st International *Conference on Microwave, Radar and Wireless Communications (MIKON 2016). Physics.* Krakow, 9-11 May 2016. pp. 1–3.
10. K. Jaldehag, C. Rieck, S.-C. Ebenhag. Time and Frequency Activities at SP in Sweden. *41st Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting*. 16-19 Nov 2009. pp. 231–252.
11. Rec. ITU-T G.8271/Y.1366 (08/2017). Time and phase synchronization aspects of telecommunication networks. Appendix V Delay asymmetry resulting from interface rate change in PTP-unaware network elements.
12. Солдатов В., Гаврилов А., Матвієнко М. та ін. Результати дослідної експлуатації підсистеми забезпечення єдиним часом військових споживачів на базі серверів точного часу Microsemi Time Provider 4100. *Український метрологічний журнал. Ukrainian Metrological Journal*. 2020. № 1. С. 68–78.

References

1. ATIS-0900005. GPS Vulnerability. Technical Report. Alliance for Telecommunications Industry Solutions. Approved September 7, 2017. 23 p.
2. Postanova Kabinetu Ministriv Ukrainy vid 2 veresnia 2015 r. № 664 "Pytannia Sluzhby yedynoho chasu i etalonnych chastot" [Resolution of the Cabinet of Ministers of Ukraine dated September 2, 2015 No. 664 "Issues of the Time Synchronization and Reference Frequencies Service "] [in Ukrainian]. URL: https://zakon.rada.gov.ua › 664-2015-п
3. Istituto Nazionale di Ricerca Metrologica (INRIM) Report to the 20th Meeting of the CCTF INRIM's Time and Frequency Activities. September 2015. 16 p.
4. Symmetricom Datasheet «Precise Time Scale System». URL: https://www.microsemi.com/product-directory/time-frequency-systems/4156-precise-time-scale-system#r 5.
5. Michael A. Lombardi et. al. Accurate, Traceable, and Verifiable Time Synchronization for World Financial Markets. Journal of Research of the National Institute of Standards and Technology. Volume 121, 2016. pp. 436-463esources
6. Oleg Ulyanov , Volodymyr Chmil, Yaroslav Yatskiv et al. Sozdanie radioteleskopa RT-32 na baze antennoy sistemi MARK-4BK-4B. 1. Proekt modernizatsii i pervie rezultati. [Creation of the RT-32 radio telescope based on the MARK-4B antenna system. 1. Modernization project and first results]. *Radiofizika i radioastronomiya - Radiophysics and Radioastronomy*. 2019. T. 24. № 2. pp. 87–116. [in Russian].
7. Viktor Gaidamanchuk. Results of development VLBI time scale system RT-32 Zolochiv. *International Workshop "RT-32 Zolochiv: First Results, EU Collaboration, Radio Astronomy Frontiers".* Zolochiv, Ukraine, 3-5 October 2021. *URL:* https://spacecenter.gov.ua/contents/uploads/2021/10/Viktor-Gaidamanchuk__Results-of-Develompent-VLBI-Time-Scale-System-RT-32-Zolochiv.pdf
8. Gerard Petit Atomic time scales TAI and TT (BIPM): Present status and prospects. *Proceedings of the 7th Symposium Frequency Standards and Metrology*. 2009. pp. 475–482.

9. Ł. Śliwczyński et. al. Remote synchronization of atomic clocks. 2016 21st International *Conference on Microwave, Radar and Wireless Communications (MIKON 2016). Physics.* Krakow, 9-11 May 2016. pp. 1–3.
10. K. Jaldehag, C. Rieck, S.-C. Ebenhag. Time and Frequency Activities at SP in Sweden. *41st Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting*. 16-19 Nov 2009. pp. 231–252.
11. Rec. ITU-T G.8271/Y.1366 (08/2017). Time and phase synchronization aspects of telecommunication networks. Appendix V Delay asymmetry resulting from interface rate change in PTP-unaware network elements.
12. Soldatov V.,Gavrilov A., Matvienko M. et al. Rezultaty doslidnoi ekspluatatsii pidsystemy zabezpechennia yedynym chasom viys’kovych spozhyvachiv na bazi serveriv tochnoho chasu Microsemi Time Provider 4100 [The results of pilot operation of the subsystem of universal time provision for military consumers based on the precise time servers Microsemi Time Provider 4100]. *Ukrainskyi metrolohichnyi zhurnal – Ukrainian Metrological Journal*. 2020. № 1. pp. 68–78 [in Ukrainian].

УДК 535.345

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОПТИЧИХ ПІДСИЛЮВАЧІВ НА СУЧАСНИХ DWDM МЕРЕЖАХ ЗВ'ЯЗКУ

DOI 10 36994 / 2788- 5518- 2022-02-04-04

Манько О О*. д.т.н., проф.Київський фаховий коледж зв'язку,Київ,Україна. manko_kiev@ukr.net*

Харлай Л. О. *к.т.н.,доц.Київський фаховий коледж зв'язку,Київ,Україна. Lharlay@i.ua*

Анотація: *В роботі наведено принципи функціонування оптичних підсилювачів, та їх конструктивної побудови. Крім того надано особливості їх використання на оптичних мережах зв'язку сьогоднішнього покоління. Показано відмінності їх побудови в залежності від специфіки поставлених завдань.*

FEATURES OF THE APPLICATION OF OPTICAL AMPLIFIERS ON MODERN DWDM COMMUNICATION NETWORKS

Oleksander Manko, *Dr.habil.,Prof. Kyiv Professional College of Communications, Kyiv, Ukraine. manko_kiev@ukr.net*

Liudmila Kharlai, *Ph.D., Ass.Prof. Kyiv Professional College of Communications, Kyiv, Ukraine. Lharlay@i.uaM*

Abstract *: The paper presents directions for the further development of modern fiber-optic communication. The need for a constant increase in the information-throughput capacity of optical communication lines, associated with the increase in the information-throughput capacity of an optical fiber, is noted. The principles of DWDM technology, which allows to meet the growing needs for increasing this capacity, are considered. The high number of regenerators on optical transmission lines for the introduction of DWDM technology was noted, and a conclusion was drawn about the expediency of using broadband optical amplifiers instead of regenerators, which amplify the optical group signal in a purely optical form, without converting it into electrical form.*

The work also shows the advantages of using optical amplifiers on transmission lines, in particular, the possibility of implementing very long systems without regenerators, but only with amplifiers. In addition, the problems that can be encountered when using optical amplifiers, and which are caused by nonlinear effects in the optical fiber, are given. A list of these effects and ways to reduce or avoid them is provided.

Types of optical amplifiers for achieving certain technical characteristics are presented. In particular, these are booster amplifiers, pre-amplifiers and linear amplifiers, the use of which is connected with the solution of certain technical problems - noise reduction, power increase, etc.

The construction of systems with the involvement of optical amplifiers, which include the complex use of amplifiers along with receiving or transmitting equipment, is shown.

Three main types of optical amplifiers are described and characterized according to the principle of operation. Namely: a fiber optic amplifier on an erbium-doped fiber, a semiconductor amplifier and an amplifier based on the effect of forced Raman scattering. A comparative analysis of their characteristics was carried out.

Conclusions have been made regarding the features of the application of various types of optical amplifiers in communication networks.

Key words: *Optical amplifier, optical fiber, stimulated emission, nonlinear effects, noise characteristics*

Вступ

Оптичне волокно має величезну інформаційно-пропускну здатність. І ще не так давно не уявлялось, що вона коли-небудь буде затребувана, але попит на обмін інформацією випередив усі очікування. Поступове підвищення швидкості передавання себе вичерпало, оскільки потенціальні можливості електроніки вже не могли забезпечити потрібну швидкодію. Найти ефективне рішення допомогла існуюча класична технологія з частотним розділенням каналів. Цей принцип був покладений в основу ідеї об'єднання оптичних сигналів декількох систем передавання в одному волокні. В якості несучої довжини хвилі для кожного каналу вибиралась

цілком визначена – така, щоб спектри сигналів в оптичному діапазоні не перетинались [1,2]. Ця технологія отримала назву WDM або DWDM в залежності від інтервалу між каналами.

Паралельно з появою нової технології з'явились проблеми, які необхідно було вирішити. Головною проблемою стала регенерація великої кількості каналів, оскільки багатоканальний груповий сигнал, насамперед, треба було розділити, потім подати кожен у своє волокно та на вхід свого регенератору. А після проведення операції регенерації знову об'єднати в одному волокні. Так як кількість регенераторів у кожному вузлі дорівнювала числу оптичних каналів, а кількість каналів досягала декількох десятків і поступово зростала – відповідно зростала і вартість лінії передавання. Необхідно було знайти ефективне вирішення цієї проблеми, і воно було знайдене з появою оптичних підсилювачів [1].

Такий важливий параметр оптичної системи передавання, як довжина регенераційної (підсилювальної) дільниці зазвичай обмежується втратами у лінійному волокні [3]. Для досить довгих оптичних ліній передавання обмеження, що вносять втрати, традиційно долається за допомогою регенераторів, в яких оптичний сигнал спочатку перетворюється в електричний струм, а потім регенерується за допомогою відповідних електронних схемних рішень. Такі регенератори стають досить складними та дорогими для систем з мультиплексуванням за довжиною хвилі (DWDM), оскільки кожен канал потребує окремого регенератора. При цьому для попереднього розділення групи каналів та подальшого об'єднання після процесу регенерації необхідна наявність демультиплексору та мультиплексору, які самі по собі є складними оптичними пристроями. Враховуючи той факт, що кількість оптичних каналів сучасних DWDM - систем перевищує декілька десятків, вартість обладнання значно зростає. Альтернативний підхід для компенсації цих втрат передбачає використання оптичних підсилювачів [4], які підсилюють груповий оптичний сигнал у визначеній смузі частот, що складається з багатьох каналів, безпосередньо, не вимагаючи його перетворення в електричний вид. Протягом 1980-х років було розроблено кілька типів оптичних підсилювачів, а використання оптичних підсилювачів для оптичних систем великої дальності отримало широке розповсюдження протягом 1990-х.

Оптичні підсилювачі (ОП) або (Optical amplifiers (OAs)) — це пристрої, засновані на принципах функціонування лазерів [5]. Вони отримують на вході груповий сигнал, що складається з ряду оптичних каналів, кожен з яких знаходиться у межах визначеного діапазону (вікна прозорості) оптичних частот, і одночасно посилюють усі канали на своїй довжини хвилі кожен.

Застосування ОП в оптичних системах передачі дає ряд переваг. Головною серед цих переваг є можливість реалізувати системи дуже великих довжин без регенераторів, а лише з підсилювачами. Розгортання ОП, ймовірно, дозволить вивести з експлуатації багато існуючих звичайних дільниць регенерації та, у випадку проектування нових маршрутів, зробить непотрібним побудову багатьох регенераційних дільниць, замінивши регенератори підсилювачами [5]. ОП також дозволяють розглядати нові архітектури оптичних систем для застосування в наземних і підводних мережах дальнього зв'язку та доступу. Двома прикладами цього є мультиплексування за довжиною хвилі та програми «точка-багато точок», підходи, які раніше вважалися надзвичайно складними та дорогими. ОП також пропонують потенційні переваги щодо варіантів оновлення мережі через їх незалежність від формату модуляції та швидкості передачі даних.

Однак застосування ОП також виявляє ризик нових потенційно серйозних загроз для нормального функціонування оптичної системи передавання, які є наслідком високих рівнів потужності сигналу на виході ОП, і великих відстаней між пунктами регенерації. Ці ефекти передавання визначаються нелінійністю оптичного волокна, ефектами поляризації та ефектами, зумовленими характеристиками підсилення самого ОП [6,7]. Хроматична дисперсія також стає все більш важливою для довгих нерегенерованих систем, з увімкненими ОП. Крім того, дисперсійні характеристики волокна впливають на рівень впливу порушень функціонування системи передавання, викликаного декількома домінуючими нелінійними ефектами.

ОП знаходять застосування як в одноканальних так і багатоканальних системах. На додаток до погіршень передавання, що мають місце в одноканальних системах, багатоканальні системи також можуть отримати погіршення параметрів передавання через певні нелінійні ефекти. Вони включають чотирихвильове змішування (Four-Wave Mixing - FWM), перехресну фазову модуляцію (Cross Phase Modulation - XPM) і, потенційно, через вимушене комбінаційне розсіювання (Stimulated Raman Scattering - SRS) [6,7]. Як наслідок, при проектуванні

багатоканальних систем необхідно вживати особливих запобіжних заходів, щоб уникнути цього шкідливого впливу або зменшити його.

Види оптичних підсилювачів

Бустерний підсилювач (Booster (power) Amplifier – BA)

Бустерний підсилювач (БП, підсилювач потужності) — це ОП-пристрій високої потужності, який використовується безпосередньо після оптичного передавача для підвищення рівня потужності його сигналу [8]. БП не потребує суворих вимог до шуму та оптичної фільтрації.

Застосування БП (часто в поєднанні з попередніми підсилювачами) є дуже привабливим, особливо в тих випадках, коли проміжні підсилювачі в лінії небажані або недоступні, як, наприклад, у підводних системах. У будь-якому випадку, менша кількість проміжних пунктів підсилення означає простіше обслуговування для оператора мережі.

Через відносно високий рівень вхідної потужності небажаний шум підсиленого спонтанного випромінювання (Amplified Spontaneous Emission - ASE) [7,8], який за своєю суттю присутній через статистичний процес генерації фотонів всередині ОП, зазвичай незначний. Однак застосування БП може призвести до порушень режиму передавання системи, спричинених нелінійністю волокна, через високі рівні оптичної потужності, створювані БП, і велику довжину інтерактивної взаємодії фотонів, яку забезпечує відповідна довжина підсилювальної дільниці.

Попередній підсилювач (Pre-amplifier – PA)

Попередній підсилювач (ПП) — це пристрій ОП з дуже низьким рівнем шуму, який використовується безпосередньо перед оптичним приймачем для підвищення його чутливості [7]. Необхідний низький рівень шуму може бути досягнутий за рахунок використання вузькосмугових оптичних фільтрів. У цьому випадку було б вигідно автоматичне налаштування центральної довжини хвилі фільтра попереднього підсилювача на довжину хвилі передавача, оскільки це дозволило б пом'якшити вимоги як до початкового допуску довжини хвилі передавача, так і до його довгострокової стабільності.

Як зазначалося раніше, використання ПП (у поєднанні з БП) є простим засобом реалізації значного збільшення енергетичного потенціалу системи передавання.

Лінійний підсилювач (Line Amplifier – LA)

Лінійний підсилювач (ЛП) — це малошумний ОП-пристрій, який використовується між регенераційними пунктами лінійного волокна для збільшення відстані між регенераторами або, у випадку з багатоточковим з'єднанням, для компенсації втрат на розгалуження в оптичній мережі доступу [7,8].

Як зазначалося раніше, лінійні підсилювачі можуть замінити деякі або всі звичайні регенератори в секціях оптоволокна на великі відстані. Можна уявити, що більш ніж один звичайний регенератор може бути замінений одним ЛП, з очевидною перевагою зменшення кількості обладнання в лініях передачі. Крім того, в майбутньому можливі ситуації, коли в міжміських мережах з'являться як лінійні підсилювачі для компенсації загасання сигналу, так і звичайні регенератори для компенсації спотворень сигналу.

Типова конфігурація ОП (як ЛП) у багатоканальній системі передавання показана на рис.1.

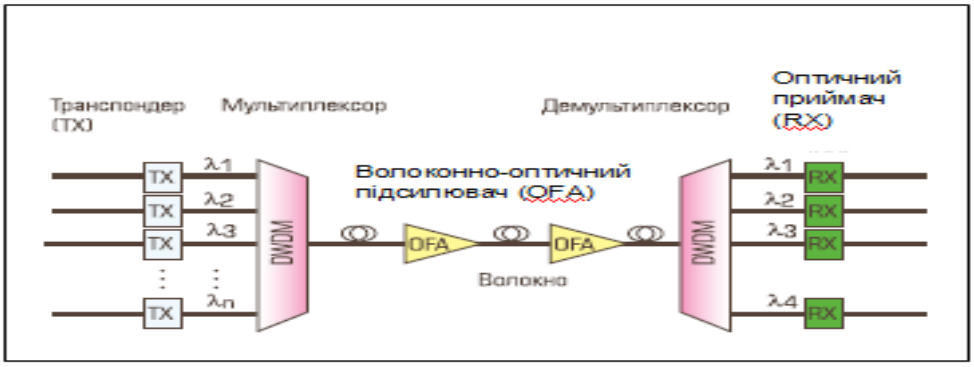


Рис.1. Лінійний підсилювач в багатоканальному застосуванні

На стороні передавання n сигналів, що надходять від n оптичних передавачів, Tx1, Tx2, . . Txn, кожен з яких має унікальну довжину хвилі, λ1, λ2, . . . λ n, відповідно, об'єднуються оптичним мультиплексором (ОМ). На приймальній стороні n сигналів на своїх довжинах хвиль - λ1, λ2, . . . λ n, розділяються оптичним демультиплексором ОД (OD) і направляються до окремих оптичних приймачів Rx1, Rx2, . . . Rxn відповідно.

Передавач з оптичним підсилювачем (Optically amplified transmitter (OAT))

Передавач із оптичним підсилювачем – ПОП (OAT) — це підсистема ОП, у якій підсилювач потужності інтегровано з лазерним передавачем, у результаті чого створюється передавач високої потужності (рис.2) [8].

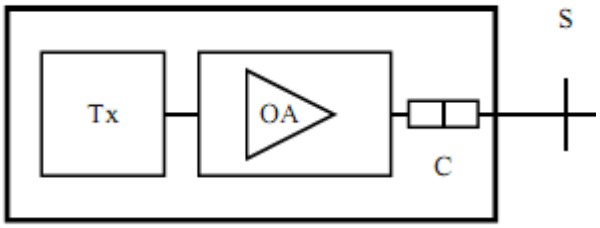


Рис. 2. Побудова передавача з оптичним підсилювачем: S - Контрольна точка в оптичному волокні після оптичного з’єднання (С) ПОП

Спосіб застосування ПОП (OAT) загалом такий самий, як і для БП.

***Приймач з оптичним підсиленням (Optically amplified receiver* – OAR)**

Приймач з оптичним підсиленням ПрОП (OAR) — це підсистема ОА, в якій попередній підсилювач інтегровано з оптичним приймачем, що забезпечує високу чутливість приймача (рис.3) [8].

Спосіб застосування ПрОП загалом такий самий, як і для ПП.

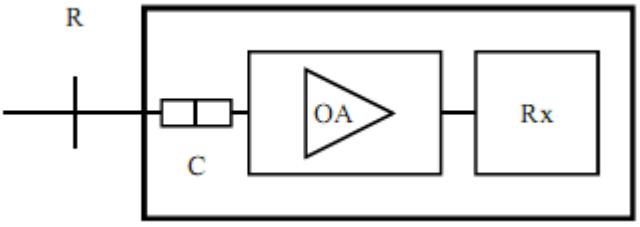


Рис.3 . Побудова приймача з оптичним підсилювачем: R Контрольна точка в оптичному волокні перед оптичним під’єднанням (С) ПрОП

Типи оптичних підсилювачів

Існує кілька типів ОП. Серед них: легований ербієм волоконний підсилювач (EDFA), напівпровідникові оптичні підсилювачі (SOA), раманівські підсилювачі [5,6]. ОП потребують електричної або оптичної енергії для переведення електронів на вищий енергетичний рівень. Енергія, як правило, забезпечується за допомогою введення електричного струму (у SOA) або оптичного випромінювання в підсилювачах EDFA та Рамана.

Підсилювачі типу EDFA (Erbium-doped fibre amplifier)

EDFA — це сегмент оптичного волокна довжиною від кількох метрів до кількох десятків метрів, до якого додається рідкоземельний елемент ербій. Іони ербію можуть збуджуватися за допомогою накачування на кількох оптичних частотах. Дві найбільш зручні довжини хвилі збудження - 980 нм і 1480 нм [3]. Коли ці довжини хвилі поширюються через активне волокно, іони ербію збуджуються, і вхідний оптичний сигнал може бути посилений стимульованим випромінюванням, вивільняючи енергію електронів для генерації фотонів у діапазоні довжин хвиль 1530-1565 нм (С-діапазон). Змінивши конструкцію підсилювача, цей діапазон також можна змістити до більш довгих хвиль (L-діапазон).

Основна структура EDFA складається із з'єднувального пристрою, волокна, легованого ербієм, і двох ізоляторів (по одному на кожному кінці) (рис. 4).

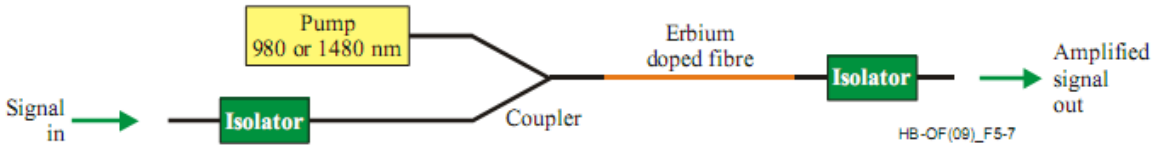


Рис.4. Приклад побудови підсилювача EDFA

Волокно, по якому передається сигнал, підключається через ізолятор, який критично зменшує відбите в зворотному напрямку світло. EDFA стимулюється лазерним джерелом, відомим як лазер накачування. Потужність накачування (на хвилях довжиною 980 нм або 1480 нм) подається в EDFA разом із вхідним сигналом даних. Накачування збуджує легуючі іони волокна, що призводить до підсилення сигналу даних, який лежить в околі довжин хвиль в області 1550 нм.

Підсилювачі типу SOA (Semiconductor optical amplifiers)

Фізичний механізм, що забезпечує підсилення в напівпровідникових оптичних підсилювачах (SOA), відрізняється в різних аспектах від вищезазначених підсилювачів EDFA. По суті, SOA — це напівпровідникові лазери без зворотного зв'язку з оптичним резонатором (грані чіпа мають покриття проти відбиття), тому інверсія населеності електронів генерується в активній області за допомогою електричного струму [4]. Стимульоване випромінювання фотонів відбувається через процеси електронно-діркової *рекомбінації з породженням нових фотонів, викликаних сигнальними фотонами (на довжинах хвиль, що входять до смуги посилення напівпровідникового матеріалу).*

Підсилювачі на ефекті Рамана (Raman amplifiers)

Підсилювачі зі стимульованим комбінаційним розсіюванням, тобто підсилювачі на ефекті Рамана (SRS) — це нелеговані волоконні підсилювачі, які використовують високопотужне накачування, щоб скористатися нелінійними властивостями звичайного оптичного волокна [5,9,10]. На рис. 5 показано, як волокно можна використовувати як раманівський підсилювач.

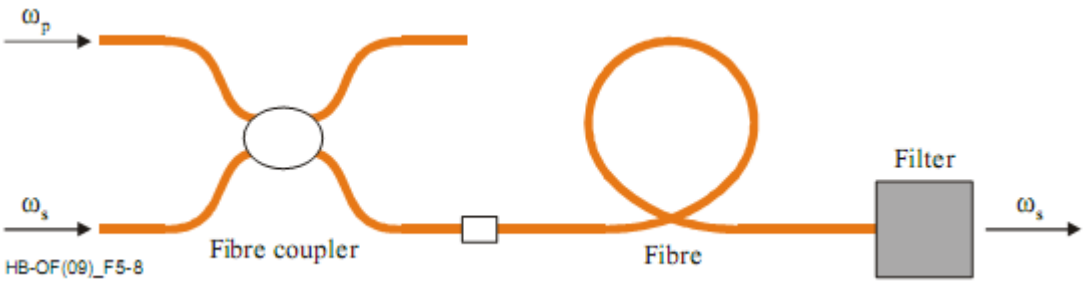


Рис.5 . Підсилювач на ефекті Рамана

Накачування та сигнал вводяться у волокно через волоконний з'єднувач. Енергія передається від сигналу накачування до інформаційного сигналу через SRS (Стимульоване раманівське розсіяння), коли два пучки спільно поширюються всередині волокна. Промені накачування та сигналу зустрічно поширюються у конфігурації зворотного накачування, яка зазвичай використовується на практиці.

Раманівські підсилювачі залежно від конструкції називають розподільними або дискретними. У дискретному випадку дискретний пристрій виготовляється шляхом намотування 1-2 км спеціально підготовленого волокна. Волокно накачується на довжині хвилі близько 1,45 мкм для посилення сигналів 1,55 мкм. У разі розподіленого Раманівського підсилення те саме волокно, яке використовується для передачі сигналу, також використовується для підсилення сигналу. Світло накачування часто інжектується у зворотному напрямку та забезпечує підсилення на відносно великих відстанях (> 20 км).

Найважливішою особливістю Раманівських підсилювачів є широкий діапазон пропускної здатності, який може поширюватися на повний корисний спектр від 1300 нм до 1600 нм без обмежень щодо збільшення пропускної здатності, яка забезпечує швидкість передавання, що перевищує терабіти за секунду [5,10]. З іншого боку, раманівське підсилення потребує лазерів накачування з високою оптичною потужністю (> 1 Вт),та з *пов'язаними з цим проблемами керування температурою, а також проблемами безпеки.*

Розподілені Раманівські підсилювачі

Розподілені Раманівські підсилювачі — це підсилювачі, у яких ефект підсилення досягається за допомогою лінійного оптичного волокна, що використовується для передавання [5]. Такі підсилювачі вважаються розподіленими, оскільки частина або все лінійне волокно використовується для підсилення. Розподілені Раманівські підсилювачі можна додатково класифікувати на три підкатегорії.

Раманівський підсилювач зі зворотним накачуванням: енергія накачування та сигнал поширюються в протилежних напрямках у лінійному оптичному волокні. Ці раманівські підсилювачі можуть розташовувати джерело накачування поблизу приймача, а випромінювання накачування розповсюджується в протилежному напрямку по відношенню до інформаційного сигналу (Рис.6, де RPi — опорна точка вхідного сигналу системи зі зворотним накачуванням, RPo — опорна точка вихідного сигналу зі зворотним накачуванням і GMP – точка вимірювання підсилення).

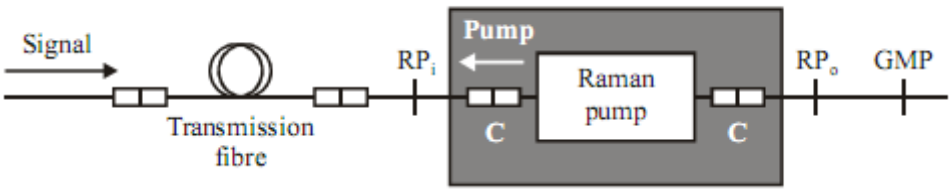


Рис. 6. Раманівський підсилювач зі зворотним накачуванням

Таким чином, накачування найсильніше біля приймача та найслабкіше біля джерела сигналу. Таке розташування має важливу перевагу: більший рівень потужності накачування знаходиться там, де він найбільше потрібний (на віддаленій відстані від джерела сигналу) і

менший рівень поблизу джерела сигналу. Отже, сигнал найбільше посилюється там, де він найслабший, і менше там, де він найсильніший.

Раманівський підсилювач із прямим накачуванням: енергія накачування та сигнал спільно поширюються вздовж оптичного волокна передавання в одному напрямку (рис.7, де FPi — опорна точка вхідного сигналу системи з прямим накачуванням, FPo — опорна точка вихідного сигналу системи з прямим накачуванням, а GMP — точка вимірювання підсилення).

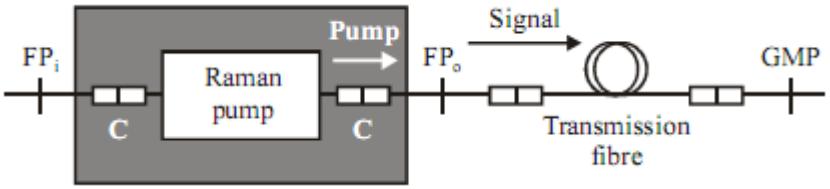


Рис. 7. Раманівський підсилювач з прямим накачуванням

Раманівський підсилювач із двонаправленим накачуванням: енергія накачування подається на обидва кінці волокна передачі.

Ця конфігурація складається з двох джерел накачування: одного на стороні передавання, а іншого на стороні приймання, причому кожне джерело працює на різних довжинах хвиль, наприклад. щоб задовольнити одночасне посилення C- та L-діапазону або реалізувати певну форму залежності вихідної потужності від довжини хвилі використовуваних каналів. У цьому випадку частина енергії накачування поширюється разом із сигналом, а частина енергії накачування поширюється проти напрямку сигналу в середовищі передачі (рис.8).

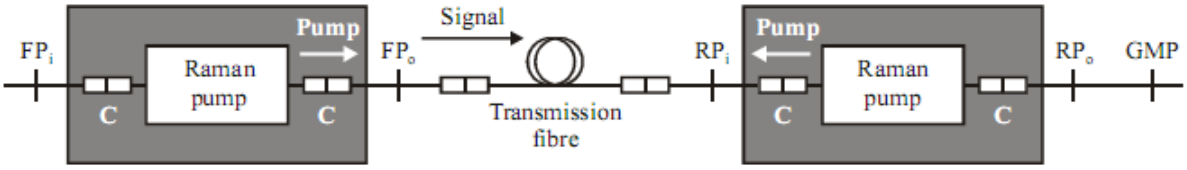


Рис.8. Раманівський підсилювач з двонаправленим накачуванням

Дискретні Раманівські підсилювачі

Дискретний раманівський підсилювач — це підсилювач оптичних сигналів, ефект підсилення якого досягається за допомогою ефекту стимульованого комбінаційного розсіювання оптичним волокном, де всі фізичні компоненти підсилювача повністю містяться всередині пристрою (Рис.9, де Ai та Ao позначають вхідні та вихідні опорні точки) [5]. У багатьох випадках використовується спеціальне оптичне волокно (крім лінійного волокна передавання), щоб зменшити необхідну потужність накачування для досягнення певного коефіцієнту підсилення.

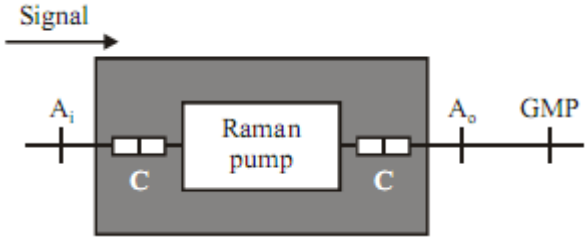


Рис. 9. Дискретний Раманівський підсилювач

Застосування EDFA, SOA та Раманівських підсилювачів

На цей час EDFA представляють собою найдосконалішу технологію OFA та поширюються на ринку протягом багатьох років і виробляються різними світовими виробниками. EDFA OA

особливо привабливий для оптичних систем DWDM і широко використовується для цих застосувань

З іншого боку, SOA все ще перебувають на стадії досліджень і розробок. Сьогодні їх виробляє дуже мало виробників, при цьому реальний вихід низький. Незважаючи на те, що технологія SOA базується на дуже добре освоєній напівпровідниковій лазерній технології, мають місце декілька важливих проблем, що пов'язані зі збиранням, обробкою, покриттям проти відблиску та поляризаційною чутливістю, ще не знайшли задовільних рішень для масового виробництва. Крім того, польові випробування SOA почалися нещодавно, і на сьогоднішній день існує лише обмежений досвід використання SOA у польових умовах. На сучасному етапі розвитку технології SOA найбільш прийнятним є застосування SOA, як блоків підсилення в оптичних системах типу «точка-точка», тобто – допоміжні підсилювачі, інтегровані з випромінюючим лазером, навіть незважаючи на деякі обмеження з точки зору вихідної потужності.

Проблеми, пов'язані з застосуванням SOA в якості лінійних та попередніх підсилювачів (такі як поляризаційна чутливість і відносно високий коефіцієнт шуму) на стадії вирішень. SOA мають великий потенціал як функціональні пристрої в оптичних комутаторах, щоб одночасно забезпечити функції підсилення та швидкого стробування, а також в інших пристроях обробки сигналів (перетворювачі довжини хвилі, оптичні мультиплексори та демультиплексори), завдяки сильній нелінійній реакції, яку вони мають у режимі насичення. Вони також можуть бути інтегровані в матриці оптичних перемикачів для компенсації внутрішніх втрат самих матриць [5].

Раманівські підсилювачі в основному використовуються в системах передавання на далекі або наддалекі відстані з дуже високою пропускною здатністю, де погіршення сигналу через шум EDFA неприпустимо або необхідна оптична смуга пропускання є більшою, ніж може підтримувати EDFA. Особливо розподілені раманівські підсилювачі можуть допомогти покращити відношення оптичного сигналу до шуму (OSNR), використовуючи волокно передачі як активне середовище [4]. Через високу вартість компонентів, спричинену високою потужністю накачування, цей тип підсилювача не встановлюється широко в сучасній мережі, але призначений для конкретних застосувань.

Висновки

Застосування волоконно-оптичних підсилювачів відкрило нову еру волоконно-оптичних технологій. Стало можливим передавання без регенераторів на відстані до 1000 км і більше. На цей час можна стверджувати, наприклад, що рішення на основі EDFA перевірені практикою, надійні, порівняно не дорогі, досить ефективні та не мають кращих альтернатив при будівництві багатоканальних (DWDM) протяжних волоконно-оптичних систем передавання з відстанню між підсилювачами порядка 60 – 120 км. В той же час Раманівські оптичні підсилювачі можуть бути ефективно використані на підводних, в тому числі морських та трансокеанських лініях.

Література

1. Слепов Н.Н. Особенности современной технологи WDM . *Электроника: Наука, технология, бизнес.* 2004. № 6. С. 68–76.
2. ITU-T Recommendation G.694.1 (06/02) Spectral grids for WDM applications: DWDM frequency grid.
3. Волоконно-оптическая техника: Современное состояние и перспективы. – 2-е изд./Сб. статей под ред. Дмитриева С.А. и Слепова Н.Н. М.: ООО «Волоконно-оптическая техника», 2005. 576 с.
4. Optical fibres, cables and systems ITU-T Manual, Geneva, 2009.
5. ITU-T Recommendation G.663, Application related aspects of optical amplifier devices and sub-systems , Geneva, 2001.
6. ITU-T Recommendation G.662, Generic characteristics of optical fibre amp, Geneva, 2009.
7. ITU-T Recommendation G.661, Definition and test methods for the relevant generic parameters of optical amplifier devices and sub-systems.
8. Андрэ Жирар. Руководство по технологии и тестированию систем WDM / Пер. с англ. под ред. А.М. Бродниковского, Р.Р. Убайдуллаева, А.В. Шмалько М.: EXFO, 2001. 251 с.
9. Скляров О.К. Волоконно-оптические сети и системы связи: Учебное СПб.: Издательство "Лань", 2010. 272 с.

References

1.Slepov N.N. Osobennosty sovremennoi tekhnolohy WDM. [Features of modern WDM technology].. Ɔlektronyka: Nauka, tekhnolohyia, byznes. 2004. № 6. S. 68–76.

2. ITU-T Recommendation G.694.1 (06/02) Spectral grids for WDM applications: DWDM frequency grid.
3.Volokonno-optycheskaia tekhnyka: Sovremennoe sostoianye y perspektyvi. [Fiber-optic technology: current state and prospects].. – 2-e yzd./Sb. statei pod red. Dmytryeva S.A. y Slepova N.N. M.: OOO «Volokonno-optycheskaia tekhnyka», 2005.576 s.
4. Optical fibres, cables and systems ITU-T Manual, Geneva, 2009.
5. ITU-T Recommendation G.663, Application related aspects of optical amplifier devices and sub-systems , Geneva, 2001.
6. ITU-T Recommendation G.662, Generic characteristics of optical fibre amp, Geneva, 2009.
8. ITU-T Recommendation G.661, Definition and test methods for the relevant generic parameters of optical amplifier devices and sub-systems.
8.Andrə Zhyrar. Rukovodstvo po tekhnolohyy y testyrovanyiu system WDM [WDM Technology and Test Guide]. Per. s anhl. pod red. A.M. Brodnykovskoho, R.R. Ubaidullaeva, A.V. Shmalko M.: EXFO, 2001. 251s.
9.Skliarov O.K. Volokonno-optycheskye sety y systemы sviazy [Fiber-optic networks and communication system] Uchebnoe SPb.: Yzdatelstvo "Lan", 2010. 272 s.

УДК 621.396.6

ВІБРАТОРНА АНТЕННА РЕШІТКА ДЛЯ МОБІЛЬНОЇ ЦИФРОВОЇ ІОНОСФЕРНОЇ СТАНЦІЇ

DOI 10 36994 / 2788- 5518- 2022-02-04-05

***Почерняєв В.М.**, д.т.н., проф. Державний університет інтелектуальних технологій і зв'язку, Київ, Україна. vpochernyaev@gmail.com*

***Магомедова М.С**, Київський фаховий коледж зв'язку, Київ, Україна. kkz.praktika@ukr.net*

***Анотація:** У статті розроблено і досліджується конструкція вібраторної антенної решітки для мобільної цифрової іоносферної станції. При виборі типу антени для мобільної цифрової іоносферної станції взято до уваги такі основні характеристики, як широкосмуговість, коефіцієнт корисної дії, ефективність прийому при малих кутах місця, надійність і простота конструкції. Показано два варіанти конструкції вібраторної антенної решітки для мобільної цифрової іоносферної станції. Вибрано варіант конструкції антенної решітки з горизонтальними вібраторами. В якості коаксіального кабелю запропоновано конструкцію, в якій внутрішній провідник має прорізі, що забезпечують широкосмуговість антено-фідерного тракту. У конструкції вібраторної антенної решітки використовується понад 20 телескопічних стрижнів замість звичайних сталевих дротів стандартної конструкції. Положенням шунта в конструкції антенної решітки, що грає роль металевого ізолятора, вдається домогтися задовільних імпедансних характеристик у широкій смузі частот. Наведено графіки залежності коефіцієнта корисної дії від кута місця для вертикального та горизонтального вібраторів. Зазначено, що у вібраторної антенної решітки декаметрового діапазону хвиль доцільно використовувати укорочені вібратори. Вібраторні антенну решітки досліджено матричним методом. Якщо уявити кожену циліндричну антенну решітку як багатополюсник, то розроблена вібраторна антенна решітка є каскадне з'єднання двох багатополюсників. Досліджено широкосмугове узгодження активних навантажень за допомогою узгоджувального трансформатора. Еквівалентна схема такого узгоджувального трансформатора враховує індуктивність розсіювання та ємності первинної та вторинної обмоток, а також ємність зв'язку між ними. Наведено графіки залежності параметру максимально-плоскої та чебишевської характеристик від значень максимального коефіцієнта відбиття та залежності максимального коефіцієнта відбиття від поточної частоти.*

***Ключові слова:** вібраторна антенна решітка, мобільна цифрова іоносферна станція, діаграма спрямованості, коефіцієнт спрямованої дії, коефіцієнт корисної дії, багатополюсник.*

VIBRATORY ANTENNA REMAINDER FOR MOBILE DIGITAL IONOSPHERIC STATION

Vitaly Pochernyaev, Dr.habil., Prof. State University of Intellectual Technologies and Communications, Kyiv, Ukraine. vpochernyaev@gmail.com

Marija Mahomedova. Kyiv Professional College of Communications, Kyiv, Ukraine. kkz.praktika@ukr.net

***Abstract:** The article develops and investigates the design of a vibrating antenna array for a mobile digital ionospheric station. When choosing the type of antenna for a mobile digital ionospheric station, such basic characteristics as broadband, efficiency, reception efficiency at small angles, reliability and design simplicity are taken into account. Two options for the design of a vibrating antenna array for a mobile digital ionospheric station are shown. The variant of the design of the antenna array with horizontal vibrators was selected. A design of coaxial cable in which the inner conductor has slots that ensure broadband antenna-feeder path is proposed. The design of the vibrating antenna array uses more than 20 telescopic rods instead of the usual steel wires of standard construction. The position of the shunt in the design of the antenna array, which play the role of a metal insulator, manages to achieve satisfactory impedance characteristics in a wide frequency band. Graphs of the dependence of the coefficient of effective action from the angle of location for vertical and horizontal vibrators are given. It is noted that it is advisable to use shortened vibrators in the vibrating antenna array of the decameter waves range. Vibrating antenna arrays were investigated by the matrix method. If you imagine each cylindrical antenna array as a multipole, then the developed vibrating antenna array is a cascade connection of two multipoles. Broadband matching of active loads using a matching transformer was investigated. The equivalent circuit of such a matching transformer takes into account the dissipation inductance and capacitance of the*

primary and secondary windings, as well as the coupling capacitance between them. Graphs of the dependence of the maximum-flat and Chebyshev parameters from the values of the maximum reflection coefficient and the dependence of the maximum reflection coefficient from the current frequency are given.

Key words: *vibrating antenna array, mobile digital ionospheric station, directional diagram, coefficient of directional action, coefficient of useful action, multipole.*

Вступ

Використання високонаправлених антенних решіток в діапазоні декаметрових хвиль дозволяє суттєво підвищити надійність та стійкість зв'язку в цьому діапазоні, зменшивши рівень завмирання сигналу на трасі іоносферного зв'язку.

Один із перспективних шляхів розвитку радіорозвідки, радіоелектронного подавлення, локації та зв'язку заснований на процесі нелінійної взаємодії потужного електромагнітного випромінювання діапазону УКХ з іоносферою Землі. Технічною реалізацією цього напрямку є створення мобільної цифрової іоносферної станції зв’язку, що використовує ефект штучної іоносферної неоднорідності (ШІН) [1]. Горизонтальний розмір ШІН визначається шириною діаграми спрямованості (ДС) антени, а вертикальний – потужністю нагріву та фоновими умовами на висоті нагріву. Для цього іоносферні станції повинні бути обладнані антенними ґратами з високим коефіцієнт спрямованої дії (КСД) та ДС із низьким рівнем бічних пелюсток. Крім цього, антенна решітка для роботи в дуплексному режимі на прийомі повинна забезпечувати сектор кутів 5^0 … 25^0 при дальностях понад 1000 км.

Така станція є станцією подвійного призначення і може використовуватись:

- у військових конфліктах і бойових діях;
- в умовах надзвичайних ситуацій, як при екологічних і техногенних катастрофах, так і при протидії загрозі тероризму;
- в інтересах трансляції TV програм на території, що тимчасово окуповані.

У ході бойових дій така мобільна цифрова іоносферна станція (МЦІС) може виконувати такі завдання:

- організація передачі циркулярних повідомлень на великі території, у тому числі на території, які непідконтрольні нашим військовим формуванням;
- встановлення радіозв’язку з *N*-кореспондентами без залучення ресурсів супутникового зв'язку (оренди каналів або стовбурів штучних супутників Землі, що не належать державі);
- постановка завад на великих територіях радіовипромінюючим засобам різного призначення та організація системи радіоелектронного подавлення;
- збирання розвідданих від радіозасобів, розміщених на великих відстанях один від одного;
- передача необхідних даних диверсійно-розвідувальним групам, розподілених на значних за віддаленістю ділянках місцевості.

При виборі типу антени для МЦІС береться до уваги широкосмуговість, коефіцієнт корисної дії (ККД), ефективність прийому при малих кутах місця, надійність і простота конструкції.

Метою роботи є розробка антенної решітки для МЦІС.

Виконання досліджень

Для МЦІС пропонується використовувати вібраторну антенну решітку, конструкція якої показана на рис 1.

Антенна решітка складається із двох циліндричних вібраторів, розташованих на двовісному причепі. На щоглі кріпляться шунти у вигляді металевих ізоляторів. Вібратори у вигляді металевих дротів діаметром декількох міліметрів кріпляться до двох кінців щогли через шунти. Утворюється циліндрична вібраторна антенна решітка, що складається з двох таких циліндрів. Кількість вібраторів для діапазону ~10МГц становить 12...16 дротів. До точки з'єднання вібраторів підводиться коаксіальний кабель. З метою забезпечення широкосмугової роботи антенної решітки внутрішній провідник коаксіального кабелю має чотири прорізи, як показано на рис.2.

Конструкція дозволяє вібраторам складатися для зручності транспортування решітки антени в мобільному варіанті станції.

Широкополосність вібратора, тобто слабка зміна його імпедансу в широкому інтервалі частот забезпечується стандартним способом - застосуванням багатодротяної конструкції великого діаметра (типу диполя Наденeнка). Зазначимо, що використання вертикального вібратора веде до зниження ККД через втрати в ґрунті. Ці втрати можна значно знизити розміщенням під антеною

решіткою металевого екрану, як показано на рис.3. Однак це суттєво ускладнить конструкцію мобільного варіанта антенної системи, тому досліджуємо вібраторну антенну решітку, показану на рис1.

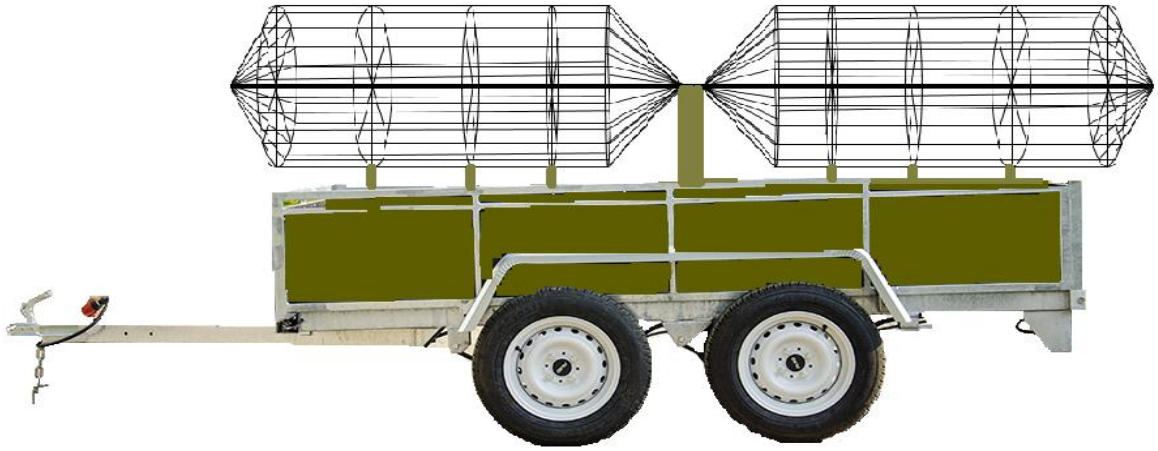


Рис.1. Конструкція вібраторної антенної решітки для МЦІС (варіант 1)

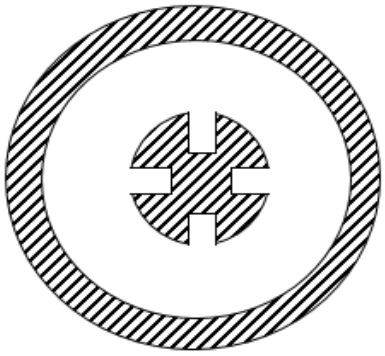


Рис.2. Поперечний переріз коаксіального кабелю антено-фідерного тракту МЦІС

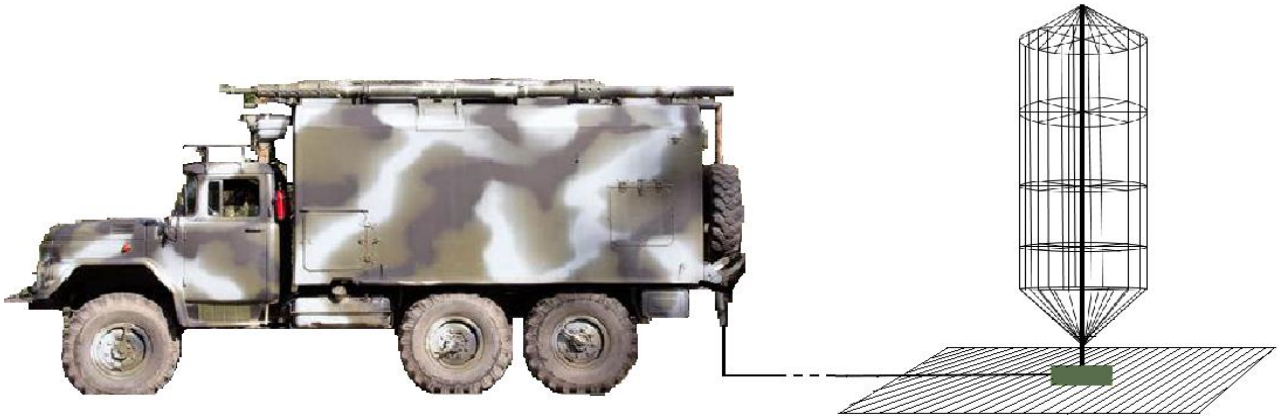
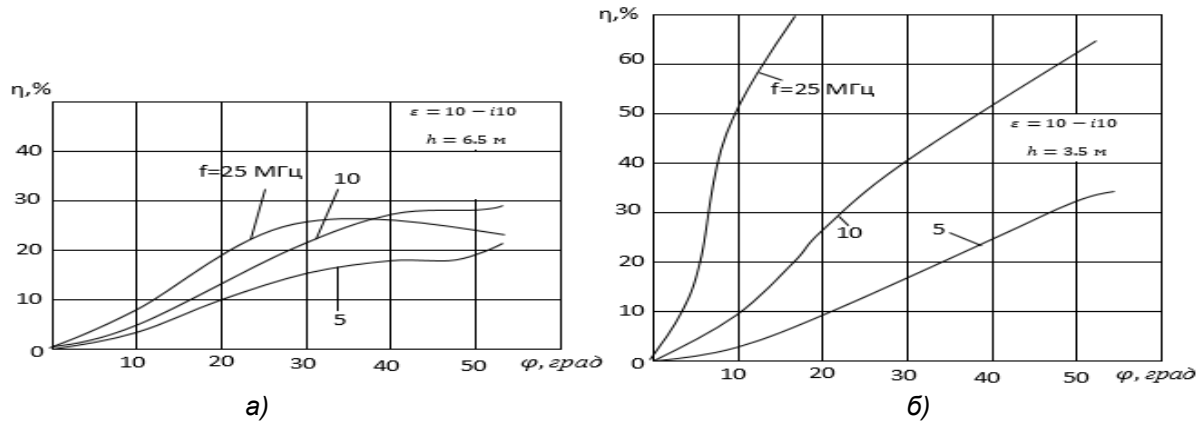


Рис.3. Конструкція вібраторної антенної решітки для МЦІС (варіант 2)

Крім того, підвищені втрати при застосуванні вертикального вібратора пов'язані з малою ефективною висотою його підвісу над поверхнею ґрунту. Наприклад, якщо висота вертикального вібратора 6,5м, то це відповідає відношенням $h/\lambda = 0{,}075$ на частоті 10 МГц та $\frac{h}{\lambda} = 0{,}2$ на частоті 25 МГц.

При дуже малих кутах місця на низьких частотах ККД антени із горизонтальних вібраторів вищі, ніж із вертикальних. Наприклад, на частоті 5МГц при куті місця $\varphi_0 = 5^0$ ККД горизонтального вібратора приблизно на 10% вище, ніж у вертикального вібратора. Також зі зростанням частоти

використання горизонтальних вібраторів дозволяє отримати істотно менше втрати за рахунок впливу ґрунту.



а) *б)*

Рис.4. Графіки залежності ККД від кута місця

На рис. 4а наведено залежності *η* (ККД) від кута місця φ_0 для вертикального вібратора: крива 1 – для частоти 5 МГц, крива 2 – для частоти 10 МГЦ та крива 3 – для частоти 25 МГц. Розмір $L \gg \lambda$ відповідає середнім параметрам ґрунту $\varepsilon' = 10 - i\,10$. На рис. 4б наведено аналогічні залежності для горизонтального вібратора. Порівняння даних рис.4 показує, що при малих кутах місця ККД антени з горизонтальних вібраторів вище, ніж із вертикальних вібраторів.

У конструкції антенної решітки на рис.1 використовується понад 20 телескопічних стрижнів замість звичайних сталевих дротів діаметром 8 мм стандартної конструкції. Положення шунта, що грає роль металевого ізолятора, вдається домогтися оптимізації імпедансних характеристик у широкій смузі частот.

У вібратора ДС описується наступним виразом:

$$f(\theta) = 4j \sin\theta \sum_{n=1}^{M} \frac{I_n}{I_1} \cos[(2n-1)\sin\theta], \tag{1}$$

де θ - напрямок головного пелюстка ДС; I_1, I_n – гармоніки струму.

Опір випромінювання вібратора запишемо так:

$$R_\Sigma = 60 \int_0^\pi f(\theta)\, f^*(\theta) \sin\theta d\theta. \tag{2}$$

Якщо втрати потужності в поверхневому опорі *Z* вібратора відсутні, то опір випромінювання знаходиться за формулою:

$$R_\Sigma = Re\, Z_a - \sum_{n=1}^{N} |I_n|^2\, Re\, Z_n. \tag{3}$$

Використовуючи формули (2) та (3) отримаємо вираз для КСД та ККД:

$$D = 30\left(k l_д\right)^2 / R_\Sigma, \tag{4}$$

$$\eta_a = R_\Sigma / Re\, Z_a, \tag{5}$$

де D- КСД; η_a- ККД; Z_a- вхідний опір; k – хвильове число; $l_д$ – діюча довжина вібратора.

Формули (1), (4), (5) описують основні електричні характеристики вібратора, що досліджується.

Зазначимо, що як випромінювач вібраторної антенної решітки метрового діапазонів хвиль доцільно використовувати укорочені вібратори. Відомо, що із зменшенням електричної довжини активна складова R_a вхідного опору вібратора падає пропорційно квадрату довжини $(l/\lambda)^2$, а реактивна X_a ємнісний характер і збільшується (за модулем) пропорційно λ/l. Узгодження вібратора зводиться до компенсації великого реактивного опору вібратора та трансформації активного опору кілька разів.

Оцінимо залежність вхідного опору $Z_{\text{a}} = R_{\text{a}} + jX_{\text{a}}$ короткого вібратора від величини індуктивного опору X_{i}. Зі збільшенням X_{i} від нуля у бік великих позитивних значень реактивна частина вхідного опору X_a переходить з області негативних в область позитивних значень через точку послідовного резонансу X_{i1}, в якій $\text{X}_a = 0$. При подальшому збільшенні X_{i} величина X_a зростає, і в точці X_{i2} спостерігається паралельний резонанс, де X_a стрибком переходить в ємнісну область і далі, асимптотично наближається до реактивного опору вібратора. Значення X_{i1} та X_{i2} залежать від $z_L\ /l$: з наближенням $z_L\ /l$ до 1 величини X_{i1} та X_{i2} зміщуються у бік великих значень, одночасно з цим зменшується різниця величин $\text{X}_{\text{i2}} - \text{X}_{\text{i1}}$. Залежність активної складової R_a має вигляд резонансної кривої і досягає максимуму в точці паралельного резонансу. Підбором скорочувальної реактивності $\text{X}_{\text{н}}$ можна компенсувати реактивну складову вхідного опору вібратора X_a і підвищити його активну складову.

З практичної точки зору найбільш цікавим є випадок, коли в плече вібратора включено навантаження $\text{X}_{\text{н}}$=$\text{X}_{\text{н1}}$, що відповідає послідовному резонансу вхідного опору. Вхідний опір є сумою збільшеного опору випромінювання і опору, зумовленого втратами в реактивності, що вкорочує. Остання складова опору не є точно опором скорочувальної реактивності, оскільки струм у точці розміщення навантаження відрізняється від струму збудження. У меншому ступені збільшення вхідного опору R_a залежить від радіусу вібратора. Так, зміна a/λ у 3 рази (від 0,001 до 0,003) призводять до зниження R_a приблизно на 20% при Q=100 та на 10% при Q=250 для $l/\lambda = 0{,}05$.

Для більшого значення R_a можна рекомендувати вибрати значення $z_L\ /l = 0{,}7 \ldots 0{,}8$, де спостерігається істотне зростанняR_a, а η_a ще незначно падає. Зменшення розмірів l/λ та a/λ, а також зменшення величини Q призводить до зниження ККД вібратора. Реально досяжна величина ККД вібратора з $l/\lambda = 0{,}05$ при застосуванні реактивності, що скорочує, з величиною Q=250 становить 35-40%. Смуга пропускання скорочувальних навантажених вібраторів оцінюється за такою формулою:

$$2\Delta f/f_0 = k^3 l^3/6\left(\ln\frac{l}{a} - 1\right) + 1/Q, \qquad (6)$$

де a – радіус вібратора. Аналіз формули (6) свідчить про те, що зменшення відношення l/λ та a/λ призводить до звуження смуги пропускання вібраторів, а укорочення вібраторів призводить до розширення смуги пропускання.

Вібраторні антенні решітки досліджуємо матричним методом. Якщо уявити кожен вібратор як багатополюсник (залежить від числа стрижнів в циліндрі), то антенна решітка (рис.1) є каскадне з'єднання двох багатополюсників.

Нехай $[S_1]$ та $[S_2]$ - матриці розсіювання двох багатополюсників, що описують дві циліндричні вібраторні антенні решітки на рис.1, з'єднаних каскадно (рис.5), а $[S]$ - матриця розсіювання всього з'єднання.

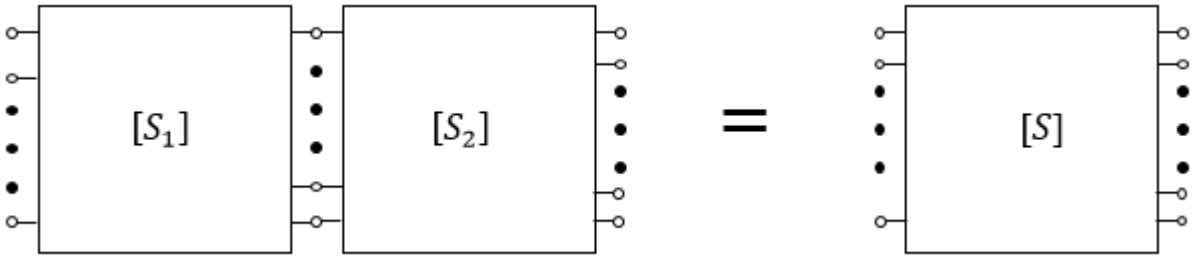


Рис.5. Каскадне з'єднання багатополюсників.

Представимо $[S_1]$ и $[S_2]$ у блочному вигляді, розбивши матриці на клітинки:

$$[S_1] = \left[\begin{array}{c|c} [R_1] & [T_1]_t \\ \hline [T_1] & [R'_1] \end{array}\right], \qquad [S_2] = \left[\begin{array}{c|c} [R_2] & [T_2]_t \\ \hline [T_2] & [R'_2] \end{array}\right],$$

Матрицю $[S]$ також зручно уявити в блочному вигляді, розділивши її на клітинки, що відносяться до першого або другого багатополюсника:

$$[S] = \left[\begin{array}{c|c} [R] & [T]_t \\ \hline [T] & [R'] \end{array}\right]. \tag{7}$$

Блоки матриці $[S]$ пов'язані з блоками матриць $[S_1]$ та $[S_2]$ наступними співвідношеннями:

$$[R] = [R_1] + [T_1]_t \{[E] - [R_2][R'_1]\}^{-1}[R_2][T_1],$$

$$[T] = [T_2]\{[E] - [R'_1][R_2]\}^{-1}[T_1], \tag{8}$$

$$[R'] = [R_2] + [T_2],\{[E] - [R'_1][R_2]\}^{-1}[R'_1][T_2]_t.$$

Підставляючи вирази (8) в (7) отримаємо розгорнутий вираз для матриці $[S]$.

Тут $[\mathrm{E}]$ - одинична матриця, порядок якої дорівнює числу з'єднань багатополюсників.

Системі випромінювачів поставимо у відповідність еквівалентний багатополюсник, який характеризуватиметься матрицею розсіювання$[S]$. В якості входу каскадного з'єднання виберемо реально існуючі входи вібраторів антенної решітки. Тоді блок матриці розсіювання повністю визначатиметься матрицею опорів [2].

Ефективне функціювання вібраторної антенної решітки в широкій смузі частот потребує відповідного узгоджувального пристрою. Формування заданого амплітудно-фазового розподілу в багатоелементних антенних решітках також вимагає узгоджувальних пристроїв, що працюють у широкій смузі частот. Одним із прикладів такого узгоджувального пристрою може бути схема, що представлена на рис.6. Така схема узгоджувального пристрою відрізняється не лише широкою смугою робочих частот, а й простотою конструкції.

Зазначимо, що формування необхідного амплітудно-фазового розподілу та в антенних решітках досягається шляхом використання відповідних узгоджувальних елементів. В якості таких елементів в діапазоні декаметрових та метрових хвиль використовуються узгоджувальні трансформатори або гібридні суматори.

Розглянемо завдання широкосмугового узгодження двох активних навантажень за допомогою трансформатора. Еквівалентна схема такого узгоджувального трансформатора враховує індуктивність розсіювання та ємності первинної та вторинної обмоток, а також ємність зв'язку між ними.

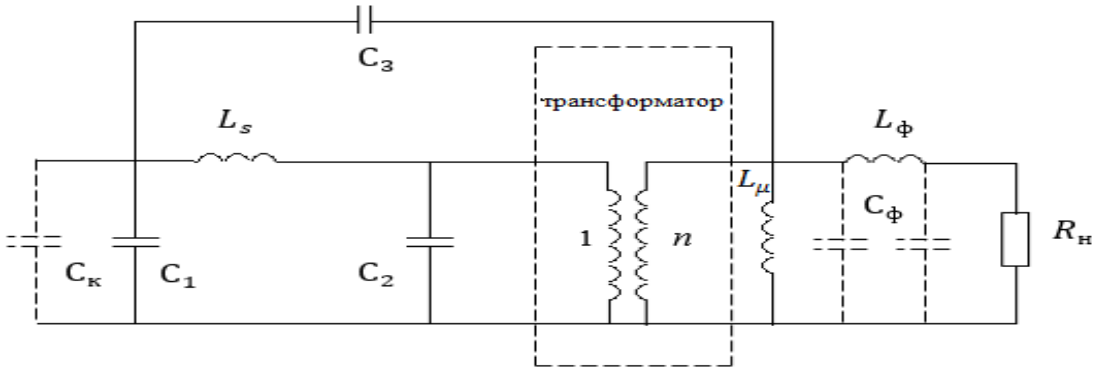


Рис.6. Схема узгоджувального трансформатора

Схема на рис.6 з достатньою для практики точністю моделює властивості як звичайних трансформаторів, так і деякі типи трансформаторів типу довгої лінії при параметрах схеми, що не залежать від частоти [3].

Приступаючи до аналізу схеми рис.6, введемо позначення: Γ – вхідний коефіцієнт відбиття при навантаженні трансформатора провідністю, що дорівнює внутрішній провідності генератора; ρ - хвильовий опір трансформатора; $\rho = \sqrt{L_s/C}$, де L_s – індуктивність розсіювання; C – власна ємність, яка дорівнює $C_1 + C_2 + C_3(n-1)^2$; $\alpha = R_н/\rho$ – коефіцієнт навантаження; f_C – частота зрізу, яка дорівнює $R_н/4\pi L_\mu$, L_μ – індуктивність намагнічування обмотки; x – поточна частота. Крім того, позначимо $m_1 = \frac{C_1}{C}$; $m_2 = \frac{C_2}{C}$; $m_3 = \frac{C_3}{C}$.

Умови, при яких забезпечується максимально широка смуга частот. Для цього випадку маємо:

$$m_1 = 0{,}5[1 + 2m_3(n-1)],$$
$$m_2 = 0{,}5[1 - 2nm_3(n-1)].$$

На рис.7 та 8 наведено залежності величини α від значень максимального коефіцієнта відбиття $|\Gamma_m|$ та $|\Gamma_m|$ від x_m, ці залежності побудовані при $nm_3 = const$ для максимально гладкої (α=1) та чебишевської ($\alpha < 1$) характеристик, причому виграш у смузі пропускання, що дається застосуванням останньої, лежить у межах 1,6 … 1,9. Ці залежності зручно використовувати під час розрахунку трансформаторів.

Практично значення m_1, m_2 і m_3 можуть залежно від конструкції та схеми змінюватися в дуже широких межах. Якщо $C_1 = k$, $C_3 = k(n-1), C = kn^3$ (C наведено до первинної обмотки, k – коефіцієнт пропорційності) і використовуючи рівність $m_1 + m_2 + m_3(n-1)^2 = 1$, отримаємо:

$$\begin{aligned} M_1 &= 1/n^3; \\ M_2 &= 3(n-1)/n^2; \\ M_3 &= (n-1)/n^3. \end{aligned} \qquad (9)$$

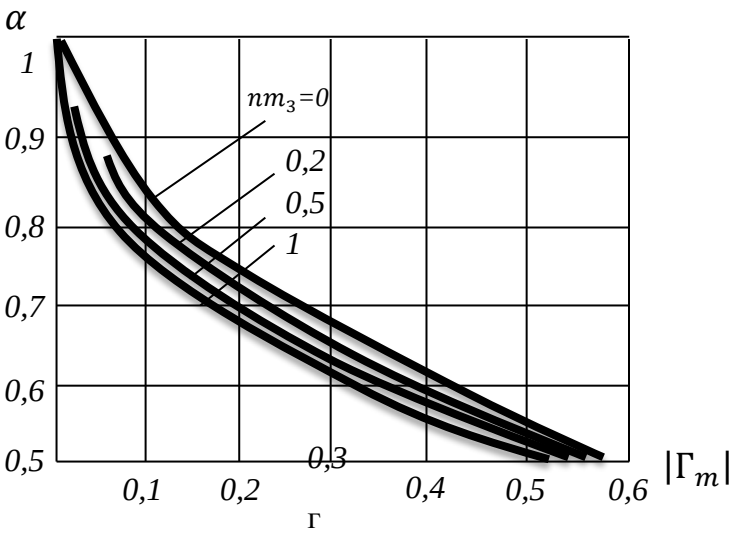
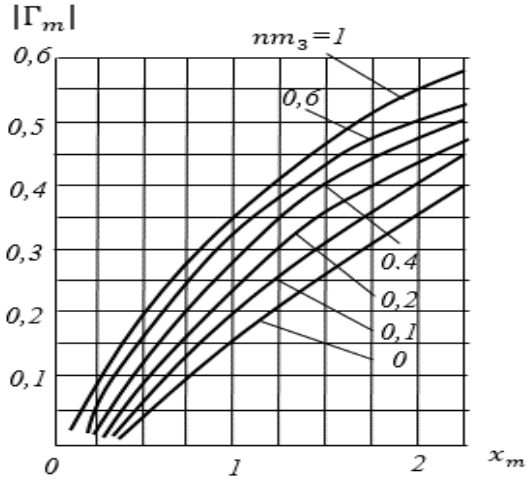
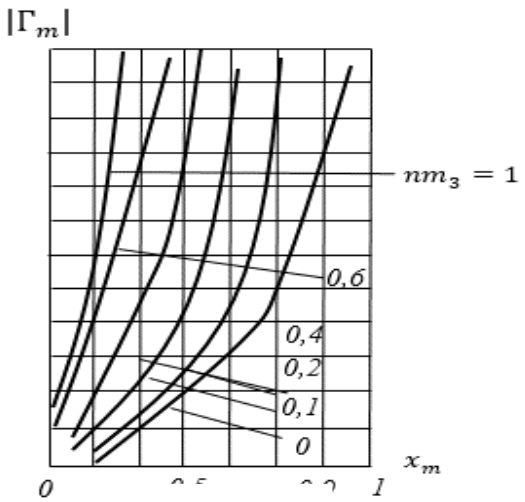


Рис.7. Графік залежності величини α від значень максимального коефіцієнта відбиття



а)



б)

Рис.8. Графік залежності максимального коефіцієнта відбиття від значень x_m

Відзначимо, що формули (9) для M_1, M_2, M_3 являються наближеними. Широкосмуговий узгоджувальний трансформатор може застосовуватися в вібраторній антенній решітки, що досліджується.

Висновки

Зазначимо, що досліджена конструкція вібраторної антенної решітки для МЦІС дозволяє реалізувати достатні для практики високі значення КСД та ККД, що відповідає результатам роботи [3]. Використання горизонтальних решіток має ширину променю приблизно $\sqrt{2\lambda/L}$, де *L* – довжина антени. Горизонтальна конструкція антенної решітки має порівняно слабку залежність ширини променю від довжини хвилі, пропорційну $\sqrt{\lambda}$ та відрізняється високою стійкістю електричних параметрів. Горизонтальна поляризація вібраторної антенної решітки декаметрових хвиль істотно ефективніша порівняно з вертикальною поляризацією для кутів місця $\varphi_0 < 10^0$.

Література

1.Почерняєв В.М., Магомедова М.С., Сивкова Н.М. Іоносферний зв'язок з використанням штучних іонізованих неоднорідностей. *Системи управління, навігації та зв'язку*, 2022. №2 (68). С.124-128.

2.Магомедова М.С., Почерняєв В.М. Широкосмуговий узгоджувальний трансформатор для антенної системи іоносферної станції зв'язку. *Scientific trends and trends in the context of globalization*: матеріали IV міжнарод. наук.-прак. конф. (Умео, Швеція 19-20 серпня, 2022р.).Швеція,2022.С.359-363.

3.Воскресенский Д.И. Антенны и устройства СВЧ. Проектирование фазированных антенных решеток. Москва: Радио и связь, 1994.412с.

References

1. Pochernyaev V.M., Mahomedova M.S., Sivkova N.M. Ionosfernyi zviazok z vykorystanniam shtuchnykh ionizovanykh neodnoridnostei. *Systemy upravlinnia, navihatsii ta zviazku [Ionospheric communication using artificial ionized inhomogeneities. Control, navigation and communication systems]*, 2022. №2 (68). pp.124-128. [in Ukrainian].

2.Mahomedova M.S., Pochernyaev V.M. Shyrokosmuhovyi uzghodzhuvalnyi transformator dlia antennoi systemy ionosfernoi stantsii zviazku. *Scientific trends and trends in the context of globalization*: materialy IV mizhnarod. nauk.-prak. konf. (Umeo, Shvetsiia 19-20 serpnia, 2022r.) *[Broadband matching transformer for the antenna system of the ionospheric communication station. Scientific trends and trends in the context of globalization: materials IV International. science-practice conf. (Umeå, Sweden, August 19-20, 2022)]*. Shvetsiia,2022.pp.359-363. [in Sweden].

3. Voskresenskyi D.Y. *Antenny i ustrojstva SVCh. Proektirovanie fazirovannyh antennyh reshetok [Antennas and microwave devices. Design of phased array antennas].* Moskva: Radio i svyaz, 1994.412p. [in Russian].

UDC 004.75

FAULT TOLERANCE REDUNDANCY METHODS FOR IOT DEVICES

DOI 10 36994 / 2788- 5518- 2022-02-04-06

Дмитренко О.А*. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. Olexandra.Dmytrenko@gmail.com*

Скулиш М.А*., д.т.н., проф, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. mskulysh@gmail.com*

Abstract: *IoT technologies are emerging with high rate. Fault tolerance influences not only the general quality of work in a conglomeration of IoT devices, but also the security of the system. It might also affect the speed of communication. This paper describes how error detection can happen. Several methods of increasing an IoT system's fault tolerance are described and compared, showing their pluses and minuses, peculiarities of application. The methods are cold, warm and hot standby, fault tolerance event manager, forward and backward error correction. The ways of how common address and virtual routing redundancy can help with performing failover and increase the guarantees of the system stability are also described*

Key words: *IoT devices, fault tolerance, faults classification, redundancy algorithms, failover*

МЕТОДИ ВІДМОВОСТІЙКОСТІ РЕЗЕРВУВАННЯ ПРИСТРОЇВ IOT

Olexandra Dmitrenko *.National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine. Olexandra.Dmytrenko@gmail.co*

Marija Skulysh, *Dr.habil., Prof. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine. . mskulysh@gmail.com*

Анотація: *IoT (Internet of Things) технології - це невеличкі прилади, які можуть підєднуватись до інтернету та часто містять сенсори, приводи (виконавчі механізми), або все разом. Розумний годинник з купою сенсорів, розумна лампа, яку можна увімкнути чи вимкнути віддалено, система зрошення рослин у тропічній теплиці, яка вмикається при занизькій вологості та передає інформацію в кінцевому рахунку в мобільний телефон щоб допомогти контролювати стан теплиці, це все приклади IoT приладів.*

Таких приладів стає все більше з кожним днем, та їх починають монтувати майже у всю техніку як в побуті, так і на підприємствах та фабриках. Відповідальність цих пристроїв не завжди критична, але є сфери, де помилки чи недостача даних з цих пристроїв є критичною або для правильності роботи алгоритмів прийняття рішень, або ж для машинного навчання та налаштування штучного інтелекту. Одна з великих ідей, яка стоїть поза застосуванням цих технологій всюди, це ідея створення розумного міста, де не треба буде персонально намагатись людям всюди встигнути та все доглянути, але догляд за по суті якістю життя містян відбуватиметься автоматично.

В даній статті наводяться особливості приладів інтернету речей, які відрізняють їх від загально відомого клієнту в клієнт-сервісному застосунку. Це маленька енергоємність, віддалене розташування від серверів чи хмари, куди завантажується інформація, а також головне, що стосується статті, це необхідність в безперервному надаванні даних а також часта неможливість повторити надсилання тих самих даних повторно.

Засновуючись на цих відмінностях, а також маючи на увазі поступовий, а не різкий спад активності застосунку заради забезпечення максимальної якості його роботи, проводиться аналіз методів надлишковості, а саме холодного, теплого та гарячого очікування, протоколу спільної надлишкової адреси та протоколу надлишковості віртуального роутингу. Також, аналізуються типи помилок та можливість зрозуміти справжню причину помилки. В статті також зазначається спосіб активації додаткового обладнання та метод слідкування за його роботою.

Метою статті є показати, які методи надлишковості придатні для роботи саме з IoT приладами.

Ключові слова: *IoT прилади, відмовостійкість, класифікація помилок, надлишкові алгоритми, відновлення системи після відмови.*

Introduction

IoT devices are the computing devices that by connecting to the Internet can exchange information with the other similar devices or connected managing applications. We can find them in smart TVs, lamps, washing machines and many other devices that compose a popular now smart home. They can also be found in enterprises. They may help in organizing work activities such as meetings, comfortable temperature in a building depending on amount of people or booking an available room. In order to facilitate device control and maintenances in the process of production in factories on assembly lines, IoT devices are also used.

For example, they can report on the need to replace some details that are getting warn out. If to adopt a robot on such an enterprise with the API to collect this information, this can eliminate need in people's involvement in production process, because the robot will be able to take the present details and repair the apparatus. Adding to this, if the process of details' ordering is standardized, no human involvement into the basic assembly line needs will be needed. This can be very helpful on the harmful production.

Nowadays, these edge devices gain much more popularity on the daily basics. A lot has to do with the idea of smart city that gains its popularity (fig. 1). The IoT devices get widespread in the agricultural sphere. There they allow easily adjust to the changes in weather and control the state of the soil and plants, turn on watering and report on the microelements and fertile that has to be added to soil for better plant growth.

Having major things depending on the quality of work of small microcontrollers reporting their information for the future analysis and decision making, it is getting hard to lose some data. For instance, if there are two channels for the information: one for the standard status and another for warning and error messages as it is described in *fault tolerance event manager* practice [1], and one channel stops sending messages. This might cause major issues in perception of the real state of things and cause wrong behavior and decision making. IoT devices won't get correct directives and will function either in the way they were programmed or in some default way. Speaking about agriculture, watering can happen during the maximum sun activity which might kill the plants.

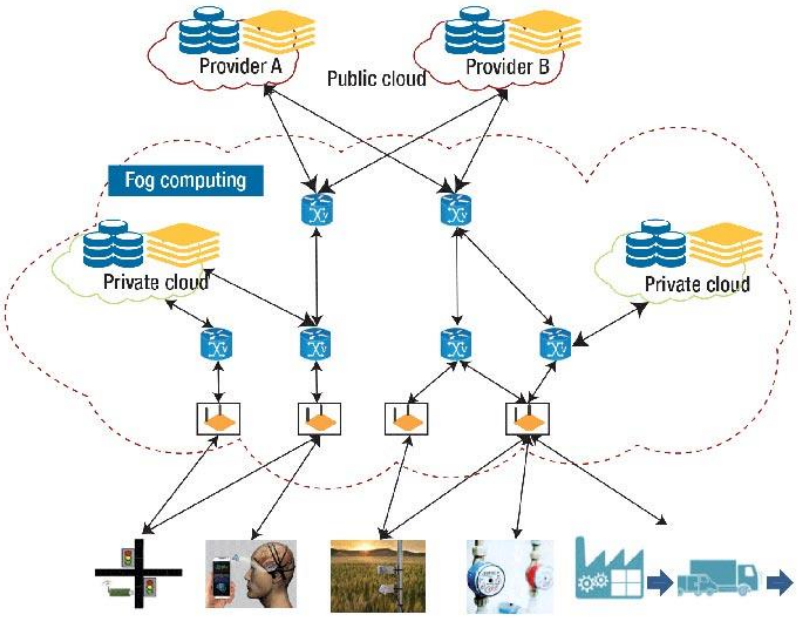


Fig.1. Distributed Systems and IOT. Source: https://www.icar.cnr.it/en/sistemi-distribuiti-e-internet-delle-cose/

This brings us to the need for *fault tolerance* [2]. Its idea is to let the system function correctly even if a fault or several took place or in the worst case *gracefully degrade*. The last means that the fall of part of the system will be obviously felt, but this won't prevent all the other parts of the system function correctly until the lacking part or its mirror is up. The main idea of this paper is to compare IoT devices with the standard clients in server-client applications, and based on the differences to propose solutions that will maximize the chances of receiving correct data on time.

Research

Peculiarities of IoT Devices Compared to Standard Clients

The question of fault tolerance is being on for many years and for sure there are many solutions on how things can be adjusted. Their present solutions were tested on systems with standard client-server applications. The question is how IoT devices are different from any other network device connected to the network.

One of the practical things is the small amount of energy being consumed during their work. It is very handy taking into consideration the sphere of application of edge devices. At the same time, having no electricity and/or no Wi-Fi, no data will be able to be sent. In order to prevent a failure of this basic level, an additional source of energy might be supplied, solar batteries and sufficient accumulators may be also placed to feed the electrical needs of a device.

Another peculiar quality is that the edge devices are often located at the distance from the reporting location. This means that there might be a need for a wired connection to the internet or for a connection to a local network through Wi-Fi. In case the connection breaks but the devices work properly, the third solution is to organize a moving connection that will come close to the devices several times a day and either read the data from the devices transmitting it further or give chance to the devices to connect to the Internet by themselves. In the case of using this technique, an IoT device has to be equipped with the proper amount of storage that will be cleaned only after the data gets transmitted.

An example of such a device is a smart ringer that records and stores all the suspicious behaviour it notices around the place. It has memory and a connection to the cloud where it transmits all the recordings. But when the connection is lost, the backup plan is to record the information on an inserted memory card and transmit it whenever the connection appears.

A different solution for having the Internet in distant places is SIM cards. As long as the carrier supports the connection in the location and the device supports SIM cards, it's possible to furnish every device with its card and be sure that if no data is received, the reason is not the network, but the malfunctioning of the device. Modern smartwatches support virtual SIM cards, so there is no need to sync the sleep information with the phone they are connected to, but sync it directly to the cloud.

The third distinguishing point of IoT devices is the regularity of the messages they send. There are many devices for measuring characteristics all the time, e.g., humidity, or recording 4k video on the streets and transmitting it to the police station. When it comes to bank robbery, which is a rare case yet possible, it's of high importance that it is discovered at its start, not when the money is already stolen and people are injured. In such institutions, it's better to have replicated devices that will preserve from a great disaster from happening.

If a device is simple and has no memory inside, which is a common case, failure to send the data results in data loss. This can break not only a single decision made based on not complete data, but ruin the system of machine learning if such is present. The process of teaching artificial intelligence is important, time and resource-consuming, so better not to repeat several times. This means that it's better to have guarantees of maximum correct data that will result in correct algorithms for future decision-making.

Below there are several methods describing how to better organize the structure of IoT devices, data from which is of high importance.

Basic Structure of IoT System and its Needs

IoT devices can communicate with each other or with the gateway, which secures the connection in between the device and the cloud or server that collects the data from all the sources and permits a connected system to make decisions based on the collected information and respond with the directives (fig. 2). Taking into consideration that some devices produce loads of information, for example, the moving of particles in an electron collider is registered every millisecond, it is getting too complicated to transmit the data as soon as it appears.

That is why there some devices perform bandwidth optimization - have integrated data processing capabilities that minimize the amount of data that has to be sent to the data centres by picking only the most important data. This technique is called *edge computing*. For example, this can be done by sending the new data only when an update happens or by sending delta in changes. This technique improves not only security footprint, taking into consideration that fewer data has to be encrypted and transferred over the network. It also reduces response time because data doesn't have to travel to and from a remote location for processing [4].

For now, there are still many unsolved issues with the security set-up. In this article, the accent is made on describing the faults that may happen in the system and possible ways how to handle them are shown.

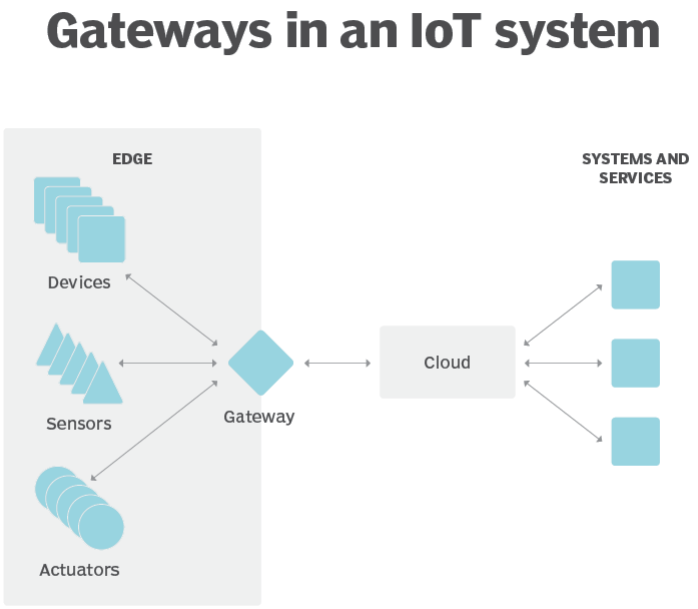


Fig.2. IoT device and Cloud management organization.

Source: https://www.techtarget.com/searchnetworking/definition/edge-device

The Faults Classification

In order to understand a cause of an error, it is important to understand the origin of an issue. If an issue is seen on a server, it could have originated not necessarily there, but possibly on any server dependency. Looking on Image 2 it can be said that if a system element fails to do its work correctly, the reason for it could be erroneous data on the cloud that could be caused by problems with the gateway or by issues with any edge or IoT devices. So basically, anything could cause an error. Below, the onion fault model is described. It contains the basic classes of faults.

The onion fault model presents the basic faults division into five main classes (fig.3). The structure describes that any upper faults reasons include any reason from the bottom layer. For example, a cause of an arbitrary fault can be a crash of a server that belongs to the fail-stop level [3].

- *Arbitrary* faults are the faults that happen once in a while, but other than that, a server works correctly.
- *Timing* - a server fails to respond in a given amount of time, but the late response would be correct.
- Omission fault is when a server doesn't respond or accept requests.
- Crash or fail-silent model of fault is when a server suddenly stops working, and it is not clear to all the working components. In synchronous systems, such faults can be detected by long timeouts.
- Fail-Stop faults happen when a server halts in the process of task execution and this gets known by relative working services.

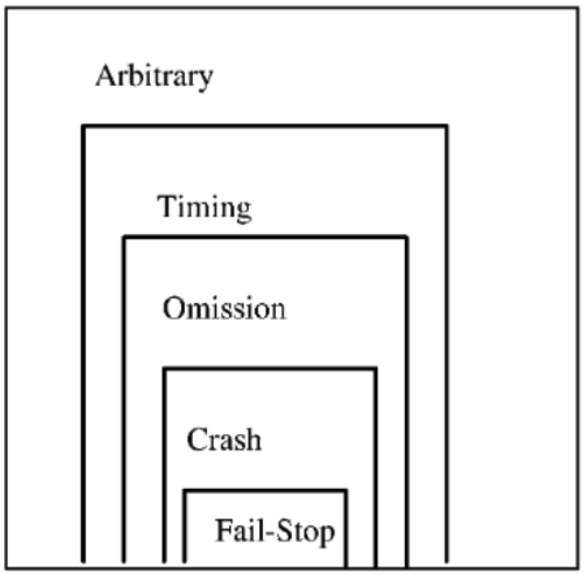


Fig.3. Onion fault model

To sum this all up, it's important to mention that at every stage there should be some guarantee that the faults won't happen because of 'stupid' reasons. If it is possible to perfect an important system with additional guarantees that a simple occasion will not destroy all the algorithms and analysis, it should be done. Below, I study the methods that may be used to prevent a basic failure and adapt them to varieties of IoT devices giving examples.

Adding Redundancy to the System

Failures can happen in any system at any moment. It's about being ready for it. Implementing a standby system might be very useful. This means that additional elements like database, servers, power or any other component will be in a ready state. In case something fails, there are other parts ready to pick up the work.

When picking a location for the standby elements, many factors should be considered. If that is a server or a database, a probability of an earthquake, war or food may be considered. This means that on one hand, it is politically more secure not to reveal user data through basing databases in other countries, but on the other hand, the probability of physical corruption should be small enough to pose a server in a nearby location.

There are several kinds of redundancy methods that may be implemented over the system depending on its needs. The methods are cold, warm and hot standbys.

Cold Standby

This is a redundancy method when another system that duplicated the running one, is installed and started once in order to be activated. After all the setup activities were done, the system is turned off and is started only in case of failure of the current working system [4].

This technique can be used in systems that either is not designed to give momentary responses to users or in the ones that don't incorporate stored data. For such systems, other standbys can fit better.

As an example of a cold standby, can serve an autonomous electricity generator that doesn't work without any need. If a sudden issue happens with the power station, so that it can no longer provide electricity, an electricity generator will turn on automatically and continue the work of the system.

Warm Standby

This technique is different from the cold standby by having the running duplicating system in parallel that time-to-time syncs data with the primary system so that in case of its fallback it will be able to pick up work and continue performing it, but only from the last back up time. If mirroring of the system is

done often, it's good for backup reliability, but the cost of mirroring should also be taken in consideration. It might be performed only at times when the system itself is not overloaded [5].

Distributed or NoSQL databases can serve as an example. Usually, applications are written in a way that servers are stateless and all the information is read from the config files or from the database. As long as replicas of the database contain the latest information, there is no issue to continuing full work from the moment and when the issue with the primary system is solved, sync all the data on the main storage.

Hot Standby

This technique is peculiar by having a duplicating system running all the time, simultaneously with the primary system. All the data is mirrored in real-time. Because of this, it is also called 'hot spare'. This is useful for systems with a high chance of failure or with a need to restart from time to time. Such a system provides not only graceful degradation but a switch on the supplementary system might not be felt by many users. Yet, often such systems are implemented in a way that when a secondary system works, it gives responses only on read-only activities. Writes are configured only on primary system which is never off for a long time [6]. A message about temporary write unavailability may be posted or the right requests might be collected in a que and performed as soon as the initial system is on and running.

Examples of such a system can be easily found in enterprise networks, as long as a second turned-on printer can serve as a replication of a primary one and perform all its activities if the user redirects the request. In a similar way, any IoT device can be replicating a base one and be ready to perform whenever it is requested by a managing system.

Hot standby reminds load balancing a lot. But is it really it? Load balancing is a technique of having two or more servers that can process the same requests. Ideally is when all the amount of the requests is divided evenly in between all the servers, so that the same number of requests will go for every server and none is overloaded [7]. Yet, this technique is not needed for IoT devices primarily because they are the source of the information and accept data only in the form of their configurations with no need to spend sufficient time on its processing.

Common Address Redundancy Protocol

The idea of a common address redundancy protocol is to share common IP address and a common virtual ID in between multiple hosts in same network segment. This conglomeration of hosts is called redundancy group. One host is a master host and it owns the IP address. Other hosts are ready to pick up if the master is not responding [8].

Virtual Router Redundancy Protocol (VRRP)

This technique is useful for cases when the physical connection with a device can break and this device will be (temporary) replaced with another having its own address. In order to eliminate issues with those, a virtual address can be used that will connect all the addressees with a working element through a virtual address, while a real one will be known only to a master router that manages all the connections. It has to be mentioned that the master router is also backed up by a group of other routers ready to take his job if it fails.

Remote measuring of water level can serve as an example of a group of devices where only one takes an action depending on its state. Several IoT devices can be set up on different height in a channel. If one of the sensors changes its state, e.g., it was flooded but now it gets not, the level of water has fallen below required and a command to open dam's gates will be sent. When water reaches another sensor, using the same IP address it sends another command which is to close the gates. There is no need for those devices to have different identifiers because they do the same function.

How to Initiate a Failover

In order for any redundancy technique to take place, in servers and IoT world the technique of heartbeats usually takes place. Working equipment sends its heartbeats with a defined regularity to a replica or to the management server. In case of any change in a regularity of the heartbeats, the

preprepared redundant equipment has to take an effect. It can be activated manually. In this case it is called 'automated with manual approval configuration'

Conclusion

This paper explains the redundancy algorithms whose main idea is to supply the network with additional either physical or logical connections or devices. Primarily, it is about determining a real cause of an issue. It is important not to take all issues too generally, but when the issue happens, have its sufficient description to eliminate problems in middleware that could possibly cause the same issue. An onion fault model describes the order of issues' severity and inclusion in one another. If an application is multipart, a substantial problem like an outage could happen with it and it will not start working by itself, but to another part of an application, it will appear as a minor issue that some indicators cannot be provided.

When a system experiences a fault, a big thing is a graceful degradation. This means that if a part of a system stopped working this shouldn't kill the whole system. All the working parts can continue supplying their functionality. When some mechanisms include the broken others to perform fully, a warning with the fault description and preferably the fix time could be shown.

In order to provide this kind of behaviour, and to cover the need for infinite non-stopping data supply from the IoT devices, the system could be supplied with additional devices that will be in standby mode waiting to be needed and turned on in the whole flow. Depending on the speed an additional device has to infiltrate and on the presence of state (memory or set up in which a working partner is), there are three types of standbys. A cold standby is when a device is initially set up and ready to participate, but is off until it will be needed. A warm standby is when one device syncs its data/state with a supplementary device. A hot standby is when a second device is in a completely ready physical and logical state to pick up work as long as sinking happens all the time.

It is not only about backup for a device. The backup should also be on the protocol level, meaning that both devices should have a common IP or virtual address or be in one redundancy group. The protocols that support this kind of addressing to different hosts are called common address redundancy protocol and virtual router redundancy protocol.

References

1. M. Melo and G. Aquino, "FaTEMa: A Framework for Multi-Layer Fault Tolerance in IoT Systems," *Sensors*, Oct. 2021. vol. 21, no. 21, p. 7181.
2. A. Sari and M. Akkaya, "Fault Tolerance Mechanisms in Distributed Systems," *International Journal of Communications, Network and System Sciences*, 2015. vol. 08, no. 12, pp. 471–482.
3. C. J. Walter and N. Suri, "The customizable fault/error model for dependable distributed systems," *Theor Comput Sci*, Jan. 2003. vol. 290, no. 2, pp. 1223–1251.
4. P. Vedavalli and C. Deepak, "Enhancing Reliability and Fault Tolerance in IoT," in *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, Jan. 2020, pp. 1–6.
5. R. Peng, Q. Zhai, and J. Yang, *Reliability Modelling and Optimization of Warm Standby Systems*. Singapore: Springer Singapore, 2021.
6. J. Wen, Y. Cao, L. Ma, and S. Du, "Design and Analysis of Double One Out of Two with a Hot Standby Safety Redundant Structure," *Chinese Journal of Electronics*, May 2020. vol. 29, no. 3, pp. 586–594.
7. [7] Jen-Hao Kuo *et al.*, "An Evaluation of the Virtual Router Redundancy Protocol Extension with Load Balancing," in *11th Pacific Rim International Symposium on Dependable Computing (PRDC'05)*, pp. 133–139.
8. [8] R. Nur, Z. Saharuna, I. Irmawati, I. Irawan, and R. Wahyuni, "Gateway Redundancy Using Common Address Redundancy Protocol (CARP)," *IJITEE (International Journal of Information Technology and Electrical Engineering)*, Feb. 2019. vol. 2, no. 3, p. 71.

УДК 621.39: 681.324

ADAPTIVE CONTROL OF SELF SIMILAR TRAFFIC IN MULTISERVICE TELECOMMUNICATION NETWORKS

DOI 10 36994 / 2788- 5518- 2022-02-04-07

***Oleksander Toroshanko**, Ph.D. Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. toroshanko@gmail.com*

***Andrii Lemeshko,** Ph. D. State University of Telecommunications, Kyiv, Ukraine. ynet@ukr.net*

***Andrii Toroshanko.** National Aviation University, Kyiv, Ukraine. atoroshanko@ukr.net*

***Abstract:** The paper analyzes approaches to increase resistance to overloads of a multi-service heterogeneous network with self-similar traffic. To solve this problem, the peculiarities of using adaptive switching systems and information distribution using Softswitch software switches and/or IP Multimedia Subsystem (IMS) software systems are considered. The test characteristics are selected and the task of testing the performance of a multi-service heterogeneous network is substantiated. Expressions are derived for describing the dynamics of changes in network quality parameters depending on the state of network nodes and network traffic statistics.*

***Key words**: multi-service network, self-similar traffic, performance tests, quality parameters, separated traffic, congestion, dynamic routing*

АДАПТИВНЕ КЕРУВАННЯ САМОПОДІБНИМ ТРАФІКОМ В МУЛЬТИСЕРВІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

***Торошанко О.С.,** к.т.н. Київський національний університет імені Тараса Шевченка, м.Київ, Україна. toroshanko@gmail.com*

***Лемешко А. В.,** д-р філос. Державний університет телекомунікацій, м.Київ, Україна. ynet@ukr.net*

***Торошанко А.І.** Національний авіаційний університет, м. Київ, Україна. atoroshanko@ukr.net*

***Анотація:** У роботі проаналізовано підходи до підвищення стійкості до перевантажень мультисервісної гетерогенної мережі з самоподібним трафіком. Обгрунтована необхідність роздільної обробки трафіку як з різними статистичними характеристиками, так і з принциповими відмінностями в структурі: трафіку "Triple Play" (мова + відео + дані), а потім "Quadro Play" (мова + відео + дані + мобільні абоненти). Для вирішення вказаної задачі розглянуті особливості використання адаптивних комутаційних систем та розподілу інформації із застосуванням програмних комутаторів Softswitch та/або програмних систем IP Multimedia Subsystem (IMS). Проаналізовані математичні моделі самоподібного мережного трафіку. Вирішується задача аналітичного визначення часових характеристик мережі, які є визначальними для досягнення максимальної швидкодії і мінімального часу доставки інформації користувачу. Для основних характеристик випадкового стаціонарного процесу (математичного очікування, дисперсії, кореляційної функції) дана оцінка точності їх визначення залежно від часу спостереження за реалізацією процесу. Виведено вирази для опису динаміки змін параметрів якості мережі залежно від стану мережних вузлів та статистики мережного трафіку.*

Розглянута концепція розподіленої інтелектуальної оцінки параметрів та стану мережі. Описана чотирирівнева архітектура сучасних телекомунікаційних мультисервісних мереж: рівень доступу, транспортний рівень, рівень управління як нова концепція комутації та рівень обслуговування, який визначає склад контенту інформаційної мережі. Вибрано тестові характеристики та обґрунтовано завдання тестування продуктивності мультисервісної гетерогенної мережі. У якості основної програми пошуку несправності вибраний двохетапний пошук, оптимальний по мінімальному середньому часу, який витрачається на виявлення відмови. Показані переваги тестів продуктивності мережі над функціональними тестами.

***Ключові слова:** мультисервісна мережа, самоподібний трафік, тести продуктивності, параметри якості, роздільний трафік, перевантаження, динамічна маршрутизація*

Introduction

The modern development of telecommunication networks (TCN) is characterized by constantly growing data transmission traffic, the organization of services is less and less related to the actual transport of information [1, 2]. This approach is the basis of the process of modernization of existing and construction of multi-service networks (MSN) of new generations.

The integration process extends not only to networks of various purposes (computer, telecommunications, document telecommunications), but also to networks with different switching methods, protocols and principles of construction [3, 4].

The relevance and perspective of the unification and convergence of networks of various purposes, the harmonization of computer and telecommunication technologies is due to the constant development of information transmission technologies and the construction of networks of new generations based on them.

The objective complexity of new generation networks is due to the use of dynamic routing principles. In addition, even in the simplest models of modern networks, we are faced with a multi-parameter system, the behavior of which we can predict only at short intervals, which, as a rule, are an order of magnitude smaller than the duration of a message divided into individual packets. The latter is caused by a change in the statistical characteristics of the traffic.

The intensity of heterogeneous traffic does not obey Poisson's or Erlang's laws. It is described by a probability distribution with so-called "heavy tails" - Pareto, Weibull, gamma distribution, etc. Such traffic is called self-similar or fractal [1, 2]. In addition, with a relatively low average intensity, instantaneous bursts (spikes) of the intensity of self-similar network traffic may occur.

During the development and implementation of modern MSN, there is an objective need for separate processing of traffic not only with different statistical characteristics, but also with fundamental differences in structure: "Triple Play" traffic (language + video + data), and then "Quadro Play" (language + video + data + mobile subscribers).

Such a task is solved with the help of SoftSwitch software switches [2, 4] and using the hardware and software complex IP Multimedia Subsystem (IMS) [5, 6]. As shown in [3], the main difference between IMS and Softswitch is the function of convergence of mobile and fixed communication. Softswitch's complex solutions allow fixed line operators to provide a wide range of services, while slightly sacrificing functions. Note that IMS platforms contain a significant number of functional modules of Softswitch platforms.

Therefore, Softswitch is usually associated with the functional structure of separate parts of the communication network that use VoIP technology, open application programming interfaces (Application Programming Interface - API) and signaling protocols (SIP, H.323, H.248, SIGTRAN). This concept is discussed in detail in many articles and books, but here I would like to note the versatile nature of SoftSwitch and the wide range of technologies that are used in SoftSwitch. The core of such systems is a software switch - the control device of the complex, the features of which work practically do not depend on the types of peripherals (terminal devices, signal and transport gateways). When using IMS, there is an opportunity for service providers, operators of fixed and mobile communications to provide services to users of all types of access networks and all types of terminals through a single network based on the IP-MPLS protocol. At the same time, the quality of telecommunication-class services is ensured, and not the "best effort" quality, as in a traditional Internet service. However, IMS can only work effectively on "pure" IP networks. Therefore, IMS should be considered as an evolutionary development of SoftSwitch hardware.

As noted above, multiservice network (MSN) traffic is by definition heterogeneous. In works devoted to the development of software switches and IMS elements, this feature and related problems are not considered. This article attempts to fill this gap.

The effectiveness of the telecommunication network management system (TCN) with packet switching is largely determined by the delays of signaling and control information, which is associated with a large number of various network switching nodes with different routing and information processing algorithms [1, 7].

Currently, there is great interest in the methods of analysis and optimization of telecommunication, computer and combined networks, intellectualization, convergence, in the implementation of network control systems that "adapt", "self-adjust", "learn", etc.

However, at the same time, there are serious gaps associated with the systematization in this area of knowledge, with the use of the mathematical apparatus of the theory, and even with the development of a sound terminology.

Such a rapid kaleidoscopic change in technologies, technical solutions and the very principles of network construction is accompanied by the closure of network equipment characteristics and, as a result, extremely low efficiency in the use of network resources [5, 8, 9]. The above leads to certain complications in evaluating the technical and economic indicators of the network, in the analysis of the influence of certain parameters of the network equipment on the efficiency of its functioning.

At the same time, theoretical science does not keep up with technological developments and attempts to quickly implement new de facto solutions. As a result, the task of analytically determining the time characteristics of the network, which are decisive for achieving maximum speed and minimum time for delivering information to the user, is complicated.

One of the key defining characteristics of TCN operation is signal and control information delays that occur during data delivery through communication channels and during processing at intermediate switching nodes [5, 7 10, 11].

The purpose of the studies covered in the article is the development of algorithms and the construction of a mathematical model for evaluating the quality of functioning, finding and determining the places of failures, overloads and emergency modes in telecommunication MSN with self-similar traffic*.*

Mathematical models of self-similar network traffic

Self-similar traffic has a special structure that does not change with multiple scaling - in the implementation, as a rule, there is a certain number of spikes with a relatively small average level of traffic [12]. Due to such bursts of load, network characteristics deteriorate: losses, delays, jitter of packets during passage through network nodes increase. Methods for calculating requirements for networks of new generations (channel capacity, buffer capacity, etc.) based on Markov models and Erlang formulas were successfully used in the design of telephone networks. Using them for modern networks with self-similar traffic can give unreasonably optimistic solutions and lead to an underestimation of the load [6, 7]. Distributions with "heavy tails" are used to describe the probability density of self-similar flows: log-normal, gamma distribution, Weibull distribution, Pareto. The latter is used to describe self-similar traffic most often [13].

Real random processes preserve the property of self-similarity only up to a certain limit. This limit or measure of statistical stability of the process at multiple scaling is determined by the so-called Hurst parameter or self-similarity parameter. A random process $x(t)$ is statistically self-similar with the Hurst parameter H $(0{,}5 \le H \le 1)$, if for any valid value $a > 0$ process $x(at)/a^H$ has the same statistical characteristics as the process itself $x(t)$:

- mathematical expectation $M[x(t)] = {M[x(at)]}/{a^H};$ (1)

- dispersion $$D[x(t)] = {D[x(at)]}/{a^{2H}};$$ (2)

- correlation function $$R(t,\tau) = {R(at), a\tau)}/{a^{2H}}.$$ (3)

The more H in (1)-(3), the longer the property of self-similarity is preserved under multiple scaling. At $H = 0.5$ this property is practically absent. Correlation functions of self-similar processes with a large Hurst parameter decay more slowly than those of ordinary random processes, and have, as a rule, an oscillatory character. It was established that the constant component of the correlation function (3) decreases according to the law:

$$c_1 t^{-c_2 a},$$

where c_1, c_2 - constants, a - scale parameter.

The expression for the probability density of the Pareto distribution has the following form:

$$f(x) = {}^{\alpha}/_{k}\left({}^{k}/_{x}\right)^{\alpha+1}, \tag{4}$$

where *k* and α (*k*, α < 0) – distribution parameters.

Accordingly, the probability function:

$$F(x) = 1 - \left({}^{k}/_{x}\right)^{\alpha} \ (x > k,\ \alpha > 1) \tag{5}$$

average value:

$$E(x) = {}^{\alpha k}/_{\alpha - 1},\ (\alpha > 1). \tag{6}$$

When transferring data of various types (voice, video, data, traffic of mobile subscribers), the so-called Quadro Play, it is necessary to take into account statistical characteristics (4)-(6) for both the case of synchronous and asynchronous service.

The concept of distributed estimation of network parameters and state

The architecture of modern TCN (Fig. 1) contains four levels [12, 13].

An access level gives users access to network resources. The transport layer is the main network resource, ensuring the transfer of information from user to user. The management level is a new switching concept based on the use of computer telephony technology and Softswitch. Softswitch technology provides a fundamentally new approach to the concept of building network nodes, call management, service provision and payment control. The level of service determines the composition of the content of the information network.

There are some fundamental differences between traditional data networks and modern smart networks. All these differences affect the principles of managing networks and their traffic. The following can be listed among the most significant differences:

1) using the principles of dynamic routing. As a result, all communication channels are quite difficult to describe and measure parameters;

2) high level of virtualization technology. New principles of differentiation of norms by parameters related to procedures for implementation of service level agreements (SLA) and even different concepts of quality of service (QoS) are applied;

3) high importance of equipment performance tests as a result, especially important principles of traffic modeling in test procedures, even at the level of field tests;

4) incomplete standardization and the lack of high-quality operational measuring equipment are currently an urgent problem. As a result, in the modern development of NGN networks, special devices and their components are used to test solutions and install equipment.

Development of the concept of distributed intelligent assessment of network parameters and state requires extensive use of analysis and monitoring systems. However, the existing management systems, despite their functional redundancy, do not have developed intellectual means in their composition, which allow to qualitatively predict the behavior of the computer network. Most management tools do not actually manage the network, but only passively monitor it. They monitor the network, but do not take active actions, recording only the fact of failure. The ideal solution would be the development of a system of analysis, forecasting and localization of possible failures in the work of both the telecommunications network in general and its individual elements. This property of the system will help to identify possible bottlenecks in advance and take measures to eliminate them in advance. However, such a control system is practically not implemented for operation in critical application conditions [2, 4].

The intelligent core of the system for forecasting the state of networks and their traffic is a control system. It is a control network and is divided into two sublevels:

The first sublevel is responsible for the state of each network element separately and is tied to specific equipment (router, bridge, switch, etc.).

The second sub-level of the control network is responsible for the general state of the controlled network segments and the network as a whole and does not depend on the equipment included in it.

This approach makes it possible to clearly separate specific equipment and the topology of the TCN. The control system automatically monitors objects in the network, collects the necessary statistical information for configuring the control network. Next, the system monitors all objects and forms a forecast of TCN performance in the future. The forecast is formed taking into account the vector of output signals of the control network.

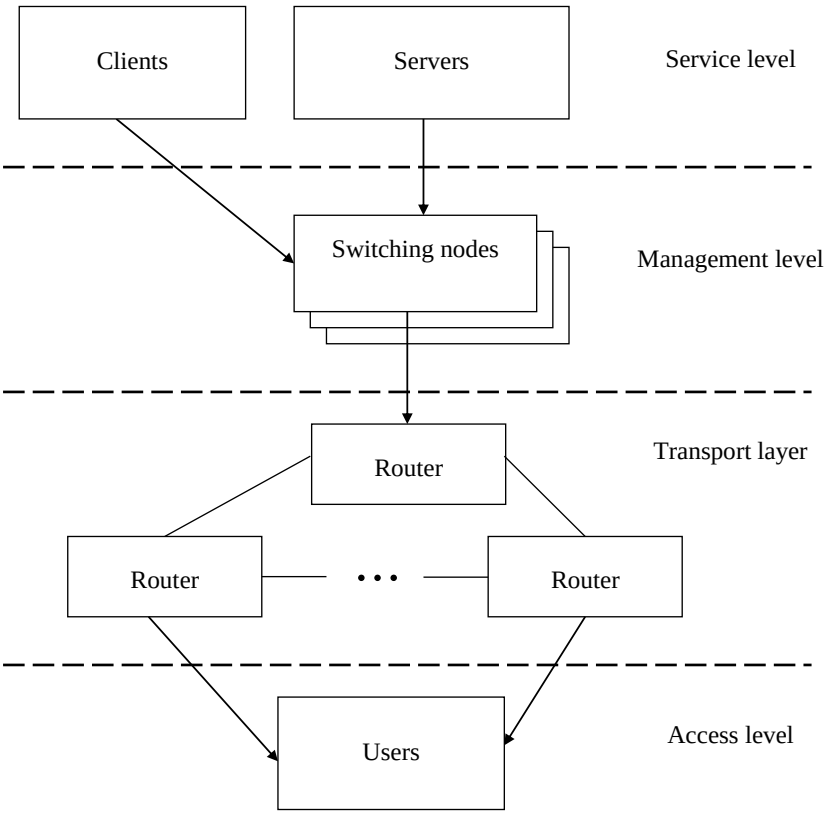


Fig. 1. Architecture levels of multi-service intelligent networks

The algorithm of the system can be divided into four main stages [14, 15]:

1) installation stage;
2) the stage of object search and collection of statistical information about the computer network;
3) stage of configuring the control network and setting its parameters;
4) network NGN monitoring stage.

The first stage is system initialization. At this stage, the initial setting of the system parameters and its self-testing take place.

At the second stage, objects are searched and statistical information about the network is collected. All received data are stored in the database of statistical information.

At the third stage, the control network is formed and configured based on the information accumulated in the database.

The first three stages are preparatory for the last, fourth stage of the algorithm's work, where there is constant monitoring of found network objects and control of the network state. The data obtained during monitoring are sent to the input of the control system. Next, a forecast of the state of each TCN object is formed, which in turn is transmitted to the input of the control system. Based on the data received at the output of the control system, a forecast of the TCN state in general is formed.

Multi-parameter problem of dynamic routing

In the case of dynamic routing of network traffic, an individual route is calculated for each packet. As a result, there is a problem of high dynamics of network settings changes. The vector of traffic parameters (profile) changes dynamically, and therefore the parameters of network nodes change. In general, the following dependence of TCN quality on network traffic parameters can be determined:

$$QoS = \Psi(\vec{L}_p), \tag{7}$$

where $\vec{L}_p = \{t_i, l_m, p_{rt}, a_c, a_{nt}\}$ - a vector of packet flow parameters;

t_i – instantaneous traffic volume;

l_m – the length of the message;

$p_{rt}, 1 \le p_{rt} \le n$ – message priority, n – the number installed by the provider priorities (the less p_{rt}, the higher the priority);

a_c – link layer address (MAC address);

a_{nt} – network address (IP address).

According to the de facto standards [6, 8] the following test characteristics for the telecommunications network:

1) capacity C_d:
   - determined by the bandwidth of the test object (device under test – DUT);
   - defines the maximum permissible load, at which there are no packet losses;
2) delivery delay L_d:
   - defines the average delay and the probability distribution of the delay;
   - packet delay is selectively measured;
3) packet losses F_l:
   - determines the frequency of packet loss in a range of data volumes and packet sizes;
   - determines the dependence of losses on the load;
4) back-to-back B_{tB} – the ability of the DUT to process frame by frame (back to back), a boolean variable «0» or «1»):
   - determines whether the DUT is capable of processing a fixed-length frame sequence;
   - the duration of work is measured τ_{cl} at the current load;
5) system Restore: determines the timeτ_{rec} DUT recovery after overload;
6) reboot: determines the time τ_{reset}, which passes from the moment of a hardware or software reset of the DUT to full operation.

As a result considering (7), we get a description of the dynamics of changes in quality parameters at each step in the following form:

$$QoS(C_d, L_d, F_l, B_{tB}, \tau_{cl}, \tau_{rec}, \tau_{reset}) = \Psi(t_i, l_m, p_{rt}, a_c, a_{nt}), \tag{8}$$

that is, a 12-dimensional state space. Considering that the entire load profile affects the quality parameters, we are faced with the impossibility of theoretically forming a complete description of the behavior of the quality parameters of the telecommunication MSM. The task is related to the multidimensional representation of the object, and the number of dimensions tends to infinity:

$$QoS(C_d, L_d, F_l, B_{tB}, \tau_{cl}, \tau_{rec}, \tau_{reset}) = \Psi(t_i, l_m, p_{rt}, a_c, a_{nt}) | \cup_{i \ne n} QoS. \tag{9}$$

This leads to another problem of MSN monitoring and analysis: even the simplest network models are multiparameter systems. Their behavior cannot be imitated with the necessary accuracy and reliability. For these reasons, all attempts to solve the problem of planning and deployment of TCN only by modeling and calculations according to (8), (9) will be clearly ineffective.

A way out of the situation can be found through a combination of theory and experiment. In particular, in conditions where quality parameters depend on the level of network load, the only method of their measurement is the combination of QoS analysis methods with the development of a detailed

model of network traffic. The numerical experiment should be carried out under different traffic intensities, varying in a wide range: from the minimum to the nominal load, and further up to peak loads and significant network overloads. It should be noted that functional testing gives a qualitative assessment of the operation of the TCN ("works - does not work"), while performance tests make it possible to give a quantitative assessment of the operation of equipment and services. These important differences of MSN testing methods from traditional networks must be taken into account first.

Conclusion

A condition for the effective functioning of TCN is stable current management in real time of all network resources, diagnostics, control of parameters and status of the network as a whole and its individual elements.

The defining task of reliability management is solved by implementing the following partial functions: network diagnostics and monitoring, identifying faulty network components and determining the type of failure, recording failures in the relevant databases, adjusting dynamic routing tables and recommending the reconfiguration of the corresponding network segment. A two-stage search, optimal for the minimum average time spent on failure detection, was selected as the main fault finding program.

For the main characteristics of a random stationary process (mathematical expectation, dispersion, correlation function), the accuracy of their determination should be estimated depending on the time of observation of the process implementation.

It is shown that functionality measurements (functional tests) become uninformative for MSN with self-similar traffic. The ratio between functional tests and performance tests is clearly changing in favor of the latter. Therefore, testing of a significant number of NGN applications and protocols must be performed at all stages of network design and deployment. From a theoretical point of view, the tasks of optimal design of modern TCN are closely related to the application of the principles of distributed management and adaptation to the current conditions of network operation.

An important prospective task of TCN reliability management is a comparative analysis of optimal and adaptive network management methods in conditions of incomplete a priori information about the state of network and terminal nodes, statistical characteristics of network traffic.

References

1. Dordal P.L. An Introduction to Computer Networks. Loyola University Chicago, Department of Computer Science, 2020. 872 p.
2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Pearson Education, Inc., Old Tappan, New Jersey, 2016. 544 p.
3. Klymash M.M., Strykhaliuk B.M., Kaidan M.V. Teoreticheskiie osnovy telekommunikatsionnykh setiei. *[Theoretical foundations of telecommunication networks],* 2014. Saarbrücken, Germany: LAP LAMBERT Academic Publishing. – 644 p. [in Ukrainian].
4. Tanenbaum A.S., Wetherall D.J. Computer Networks. Prentice Hall, Cloth, 2011. 960 p.
5. Vinogradov N.A., Drovovozov V.I., Lesnaia N.N., Zembitskaia A.S. Analiz nagruzki na seti peredachi dannykh v sistemakh kritichnogo primeneniia. [Analysis of the load on data transmission networks in critical systems]. *Zvyazok – Communication*, 2006. № 1 (61). pp. 9–12 [in Russian].
6. Benchmarking Methodology for Network Interconnect Devices : RFC 2544. URL: https://www.ietf.org/rfc/rfc2544.txt
7. Vinogradov N. A. Analiz potentsialnykh kharakteristik ustroistv kommutatsii i upravleniia setiami novykh pokolenii [Analysis of the potential characteristics of devices for switching and managing networks of new generations]. *Zvyazok – Communication*, 2004. №4. pp. 10–17 [in Russian].
8.Benchmarking Terminology for Network Interconnection Devices: RFC 1242: URL: https://www.ietf.org/rfc/rfc1242.txt
9. Ye Ouyang, Mantian Hu, Alexis Huet, Zhongyuan Li.. Mining Over Air: Wireless Communication Networks Analytics. Springer International Publishing AG, 2018. 196 p.
10. Vinogradov N., Stepanov M, Toroshanko Ya., Cherevyk V. Development of the control method of telecommunication network overload on the basis of the neural model. *Vostochno-Yevropeiskii zhurnal peredovykh tekhnolohii – Eastern European journal of advanced technologies* , 2019. №2/9(98). pp. 67–73 [in English].
11. Vinohradov N., Stepanov M., Hladkykh V., Toroshanko O. Eliminate Application Redundancy Using Local Processing Using Directional Diffusion with Mobile Agents. *Advanced Information and Communication Technologies (AICT).* 3rd IEEE International Conference, Lviv, Ukraine. 2-6 July, 2019. Lviv, 2019. pp. 360–364 [in English].
12. Yakymchuk N.M., Toroshanko A.I. Metody identyfikatsii ta kompleksnoi diahnostyky telekomunikatsiinykh system [Methods of identification and comprehensive diagnostics of telecommunication systems]. *Zbirnyk naukovykh prats Viyskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka – Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University*, 2020. №69. pp. 58–65 [in Ukrainian].

13. Valerii Kozlovsky, Nataliia Yakymchuk, Andrii Toroshanko. Comparative evaluation of Puasson's and self-similar traffic of telecommunications networks. *Infokomunikatsiini ta kompiuterni tekhnolohii – Infocommunication and computer technologies*, 2021. №2(21). pp. 41–50 [in English].

14. Toroshanko O.S. Bahatokrokova model prohnozuvannia ta vyiavlennia perevantazhennia telekomunikatsiynoii merezh [A multi-step model for prediction and detection of telecommunication network congestion] *Telekomunikatsiini ta informatsiini tekhnolohii – Telecommunications and information technologies*, 2019. № 2(63). pp. 29–37 [in Ukrainian].

УДК 621.396

МЕТОДИ ОЦІНКИ ПАРАМЕТРІВ РУХУ МАНЕВРУЮЧИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В ІНФОКОМУНІКАЦІЙНИХ СЕНСОРНИХ МЕРЕЖАХ

DOI 10 36994 / 2788- 5518- 2022-02-04-08

Цуканов О. Ф., *к.т.н., доц. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. cukanov-o@ukr.net*

Якорнов Є. А., *к.т.н., проф. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, yakornovits@gmail.com*

Анотація: *Розглянуто методи оцінки параметрів руху безпілотних літальних апаратів, що знаходяться у складі інфокомунікаційної сенсорної мережі та здійснюють різкий маневр або постійно маневрують. Для підвищення точності оцінювання параметрів руху запропоновано використовувати дробові ряди Тейлора, які в даний час мало вивчені і ще не знайшли належного практичного застосування при описі складних динамічних процесів в різних технічних додатках. На основі математичного моделювання проведено порівняльну оцінку дробових поліномів з поліномами Чебишева та поліномами на основі ряду Тейлора, яка показала, що використання дробових многочленів в «ковзному вікні» дозволяє оцінити не тільки зміни координат і швидкостей, але і фактично дає можливість підвищити точність оцінок координат параметрів руху безпілотних літальних апаратів, які постійно маневрують. Причому найбільш прийнятним многочленом для оцінки є многочлен з дробовими ступенями рівними 0,5 і, на наш погляд, необхідне подальше дослідження поліномів з дрібними ступенями вище ступеня 1,5.*

Ключові слова: *інфокомунікаційна сенсорна мережа, безпілотні літальні апарати, параметри руху, вектор стану, метод найменших квадратів, фільтр Калмана, дробові ряди Тейлора, поліноми Чебишева, інтервал «ковзаючого вікна».*

METHODS FOR EVALUATING THE MOTION PARAMETERS OF MANEUVERING UNMANNED AERIAL VEHICLES IN INFO-COMMUNICATION SENSOR NETWORKS

Oleg Tsukanov*, Ph.D., Ass. Prof. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine. cukanov-o@ukr.net*

Yevgenii Yakornov*, Ph.D..Prof. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine. yakornovits@gmail.com*

Abstract: *Methods for assessing the motion parameters of unmanned aerial vehicles that are part of the infocommunication sensor network and make a sharp maneuver or constantly maneuver are considered. Toimprove the accuracy of estimating the motion parameters of unmanned aerial vehicles, a mathematical method is proposed based on the use of the capabilities of fractional Taylor series, which are currently little studied and have not yet found proper practical application in the description of complex dynamic processes in various technical applications.*

Based on the results of research and mathematicalmodeling, a number of results were obtained, consisting in the following. For high-precision determination of the coordinates of the motion parameters of unmanned aerial vehicles, it is possible to use algorithms based on the Kalman-Busey filter or the method of least squares with a well-known motion model, since therelative accuracy of estimating these methods is almost the same, and about It is optimal to use these methods simultaneously: first, the method of least squares to obtain an estimate of measurements, and then the Kalman-Busey filter to estimate directly the parameters of motion. However, in order to assess the motion parameters of constantly maneuvering aircraft, it is necessary to use estimation methods based on a sample of measurements in a "sliding window". Anequal evaluation using algebraic polynomials, Chebyshev polynomials and fractional polynomials by the method of least squares "in a sliding window" showed

that the useof fractional polynomials makes it possible to evaluate not only changes in coordinates and velocities, but also with the help of fractional derivatives, which occupy an intermediate position between the coordinates, the first and second derivatives. , allows you to improve the accuracy of estimates of the coordinates of the motion parameters of maneuvering unmanned aerial vehicles.

Moreover, the most acceptable polynomial for evaluation is a polynomial with fractional degrees equal to 0.5. and the authors' opinion is expressed on the continuation of studies with degrees above 1.5.

Key words: *infocommunication sensor network, unmanned aerial vehicles, motion parameters, state vector, least squares method, Kalman filter, fractional Taylor series, Chebyshev polynomials, "sliding window" interval.*

Вступ

Літаючі сенсорні мережі на основі безпілотних літальних апаратів (БПЛА) знаходять дедалі ширше застосування в інфокомунікаційних системах підвищеної живучесті [1,2]. Одним із завдань, з яким доводиться стикатися розробникам, при створенні таких мереж, є визначення параметрів руху (ПР) таких БПЛА з високою точністю за наявності дестабілізуючих польотних факторів, таких як вітер (ударна хвиля при веденні бойових дій), зміна атмосферного тиску залежно від висоти польоту та інших. Тому для таких БПЛА траєкторію їхнього польоту слід розглядати як траєкторію об'єкта зі складним видом маневру і що складається з безлічі ділянок, кожна з яких необхідно описувати своєю системою диференціальних рівнянь, тобто характер його переміщення в просторі є траєкторією, на якій можна виділити ділянки з рівномірним рухом, різким маневром та ділянки з безперервним маневруванням об'єкта. Розглянемо підходи оцінки ПР для другого та третього випадків.

Виконання досліджень

Математичну постановку завдання оцінювання ПР БПЛА при їх квазіоднорідному розподілі у просторі сформулюємо в такий спосіб. На підставі наявної інформації про координати $\widetilde{x_i}$, $\widetilde{y_i}$, $\widetilde{z_i}$, та їх середньоквадратичні помилки (СКО) $\widetilde{\sigma x_i}$, $\widetilde{\sigma y_i}$, $\widetilde{\sigma z_i}$, визначити ПР - оцінки вектору стану (ВС) $\widehat{X_n}$ координати $\widehat{x_i}$, $\widehat{y_i}$, $\widehat{z_i}$, похідних (швидкостей) $\widehat{\dot{x}_i}$, $\widehat{\dot{y}_i}$, $\widehat{\dot{z}_i}$ і кореляційної матриці помилок (КМП), оцінки координат елементів K_n і надалі після чергового етапу вимірювань відстаней між сусідніми БПЛА проводити їх уточнення.

Координати БПЛА можуть бути визначені як за допомогою датчиків GPS встановлених на всіх БПЛА так і шляхом взаємного вимірювання відстаней D_{ij} між i-тим і j-тим БПЛА (рис. 1), наприклад, з використанням протоколів IEEE 802.15.4 ZigBee, 6LoWPAN, Thread , RPL [3], (у разі датчиками GPS оснащуються лише 3-4 БПЛА мережі).

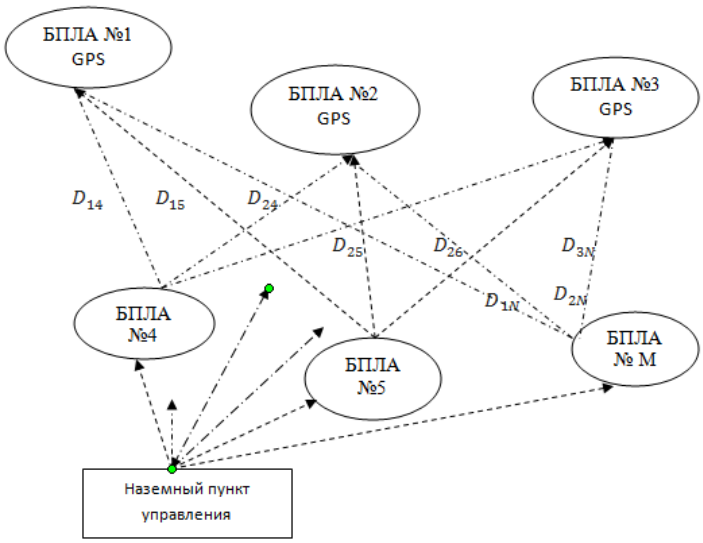


Рис. 1. Конфігурація угруповання БПЛА

Для отримання високоточних оцінок ПР у разі маневру БПЛА за багаторазових вимірів скористаємося алгоритмом оцінювання на основі фільтра Калмана [4]. При цьому припускаємо,

що помилки визначення координат, які, у свою чергу, є вхідною інформацією для алгоритму уточнення розташування елементів інфокомунікаційної сенсорної мережі, мають закон розподілу помилок, який у загальному випадку відрізняється від нормального. Для цього випадку застосування модифікованого алгоритму динамічного оцінювання на основі фільтра Калмана дозволяє, на наш погляд, отримати як стійкі оцінки ПР, так і забезпечити їхню високу точність.

Початковими умовами алгоритму оцінювання є ВС X_{n-1} та апріорна КМО K_{n-1} на *n*-1 кроці вимірювань.

Вектор стану можна записати у вигляді:

$$\mathrm{X}_{in}{}^{\mathrm{T}} = |x_{in},\ \dot{x_{in}},\ y_{in},\ \dot{y}_{in}, z_{in}, \dot{z_{in}}|. \quad (1)$$

Вектор вимірів представляється як:

$$\mathrm{Y}_{in}{}^{\mathrm{T}} = |\widetilde{x_{in}}\ ,\ \widetilde{y_{in}},\ \widetilde{z_{in}}|\ , \quad (2)$$

величини якого визначаються шляхом виміру відстаней між БПЛА.

При цьому екстрапольоване значення ВС у загальному вигляді можна подати таким чином:

$$X_{\mathrm{in}}^{\mathrm{e}} = F_{in,n-1}X_{in-1} + G_{n-1}U_{n-1}, \quad (3)$$

де $F_{in,n-1}$ - матриця екстраполяції виду

$$F_{in,n-1} = \begin{matrix} 1 & \Delta t & 0 & 0 & 0 & 0 \\ 0 & 1 & \Delta t & 0 & 0 & 0 \\ 0 & 0 & 1 & \Delta t & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{matrix};$$

G_{n-1} – матриця управління

$$G_{in,n-1} = \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \Delta t^{\,2}/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \Delta t^{\,2}/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \Delta t^{\,2}/2 \end{matrix};$$

$U_{\mathrm{n-1}}{}^{T} = |0 \quad 0 \quad 0 \quad a_{x,n-1} \quad a_{y,n-1} \quad a_{z,n-1}|$ – вектор управління;

Δt – час між вимірами відстані між БПЛА;

$a_{x,n-1} \quad a_{y,n-1} \quad a_{z,n-1}$ – прискорення БПЛА за координатами.

Якщо позначити S_{n-1} – як КМП вектор управління, то уточнене значення апріорної КМО вектор управління можна записати у вигляді:

$$S_{n-1}^{*} = S_{n-1}\gamma, \quad (4)$$

де γ – параметр стійкості процесу оцінювання.

За аналогією з (3) екстраполіровану апріорну оцінку КМП можна також подати наступним чином:

$$K_{in}^{e} = F_{in,n-1}\ K_{in-1}F_{in,n-1}{}^{\mathrm{T}} + \mathrm{G}_{\mathrm{n-1}}S_{n-1}^{*}G_{\mathrm{n-1}}^{T}, \quad (5)$$

де K_{in-1} – екстраполірована апріорна КМП.

Для подальших викладок визначимо матричний коефіцієнт посилення:

$$H_{in} = K_{in}^{e}(K_{in}^{e} + \mathrm{Q}_{in})^{-1}, \quad (6)$$

де Q_{in} – КМП вектору вимірювань Y_{in}, на n-му кроці.

Тоді оцінку ВС, подану у вигляді $\widehat{X_{in}} = |\widehat{x_{in}},\ \widehat{\dot{x}_{in}},\ \widehat{y_{in}},\ \widehat{\dot{y}_{in}},\ \widehat{z_{in}},\ \widehat{\dot{z}_{in}}|^{\mathrm{T}}$, можна в загальному випадку надати як:

$$\widehat{X_{in}} = X_{in}^{e} + H_{in}(Y_{in} - X_{in}^{e}), \tag{7}$$

а апостеріорну КМП оцінювання:

$$\widehat{K_{in}} = K_{in}^{e} - K_{in}^{e}\ H_{in}. \tag{8}$$

При цьому $\widehat{K_{in}}$ у розгорнутому вигляді представляємо матрицею виду:

$$\widehat{K_{in}} = \begin{matrix} \sigma x^2 & s_{x\dot{x}} & s_{xy} & s_{x\dot{y}} & s_{xz} & s_{x\dot{z}} \\ s_{y\dot{y}} & \sigma\dot{x}^2 & s_{\dot{x}y} & s_{\dot{x}\dot{y}} & s_{\dot{x}z} & s_{\dot{x}\dot{z}} \\ s_{xy} & s_{\dot{x}y} & \sigma y^2 & s_{y\dot{y}} & s_{yz} & s_{y\dot{z}} \\ s_{x\dot{y}} & s_{\dot{x}\dot{y}} & s_{y\dot{y}} & \sigma\dot{y}^2 & s_{\dot{y}z} & s_{\dot{y}\dot{z}} \\ s_{xz} & s_{\dot{x}z} & s_{yz} & s_{\dot{y}z} & \sigma z^2 & s_{z\dot{z}} \\ s_{x\dot{z}} & s_{\dot{x}\dot{z}} & s_{y\dot{z}} & s_{\dot{y}\dot{z}} & s_{z\dot{z}} & \sigma\dot{z}^2 \end{matrix}.$$

Тут $\sigma x^2, \sigma y^2, \sigma z^2$ - дисперсії помилок по координатах, $\sigma\dot{x}^2, \sigma\dot{y}^2, \sigma\dot{z}^2$ – дисперсії помилок по швидкостям, а s_{ab} - взаємні кореляційні моменти. Зауважимо, що склад вектору вимірювань Y_{in} та вектору стану X_{in}^{e} однаковий, тому матриця вимірювань поодинока і не показана.

Наведені вище вирази (3) - (8) і є основою пропонованого стійкого алгоритму оцінювання вектору $\widehat{X_{in}}$ і КМП $\widehat{K_{in}}$ кожного БПЛА. Ця оцінка проводиться щоразу, як у сенсорної мережі БПЛА вимірюються відстані та його помилки до сусідніх БПЛА. Як модель руху приймаємо гіпотезу про рух БПЛА із постійним значенням прискорення між сеансами визначення координат.

Розглянутий алгоритм оцінювання (3)-(8) дозволяє забезпечити стійке оцінювання ВС при раптовій зміні траєкторії руху БПЛА. Оцінки вектору стану БПЛА включають координати $|\widehat{x_{in}},\ \widehat{y_{in}},\ \widehat{z_{in}},\ |^{\mathrm{T}}$. При цьому помилки визначення координат σx_i , σy_i , σz_i і без урахування кореляційних моментів можуть бути графічно представлені у вигляді прямокутного паралепіпеда в центрі якого знаходиться БПЛА.

Аналогічно - за швидкісними складовими ВС $|\widehat{\dot{x}_{in}},\ \widehat{\dot{y}_{in}},\ \widehat{\dot{z}_{in}}|^{\mathrm{T}}$ також можна подати у вигляді паралепіпеда але з великими розмірами за абсолютними величинами. Якщо "обсяг" таких паралепіпедів буде досить малим, можна говорити про стійке автосупровід кожного БПЛА з високою точністю. Якщо такого високоточного автосупроводу не потрібно, тоді оцінюються лише координати розташування.

Стійкість оцінювання ВС БПЛА забезпечимо "примусовим збільшенням" значень діагональних елементів $\sigma\dot{a}_x{}^2, \sigma\dot{a}_y{}^2, \sigma\dot{a}_z{}^2$ матриці $G_{in,n-1}$ в (3) шляхом множення на параметр *γ*. Ця операція, у свою чергу, призводить до обмеження знизу значень елементів матричного коефіцієнту посилення $\widetilde{K_{i-1n}}$ в (8). Таким чином, константами в алгоритмі є параметр *γ* і величина *Δt*. У зв'язку з цим, при моделюванні можна заздалегідь поставити елементи КМП вектору управління S_{n-1}^{*} (4) для забезпечення стійкості та необхідної точності оцінювання.

Для перевірки запропонованого алгоритму використовувалася модель руху БПЛА на основі реальних технічних характеристик БПЛА типу "Орлан" [5], яка описувалася алгебраїчним поліномом 5-го ступеня за координатами:

$$\hat{Z}_t = a_0 + a_1\ t_{i-1} + a_2\ t_{i-1}{}^2/2 + a_3\ t_{i-1}{}^3/6 + a_4\ t_{i-1}{}^4/24 + a_5\ t_{i-1}{}^5/120, \tag{9}$$

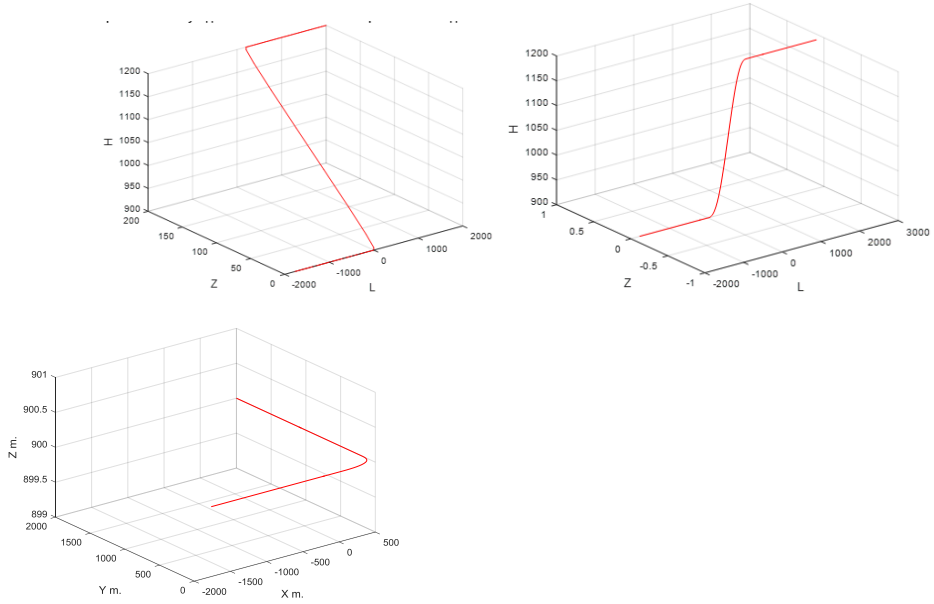
поліномом 4-го ступеня за швидкостями:

$$\widetilde{\dot{Z}}_t = a_1 + a_2\ t_{i-1} + a_3\ t_{i-2}{}^2/2 + a_4\ t_{i-1}{}^3/6 + a_5\ t_{i-1}{}^4/24 \tag{10}$$

і поліномом 3-го ступеня за прискореннями:

$$\tilde{\tilde{Z}}_t = a_2 + a_3\, t_{i-2} + a_4\, {t_{i-2}}^2 + a_5\, {t_{i-1}}^3/6\ . \qquad (11)$$

Деякі результати моделювання траєкторій польоту БПЛА за його прямолінійному русі з маневрами представлені на рис. 2, а оцінювання роботи алгоритму під час розвороту на 90^0 для різних значень параметра γ - в табл. 1.



а) б) в)

Рис. 2. Траєкторії польоту БПЛА з маневрами: а) уникнення лобового зіткнення; б) набір висоти; в) плавний розворот на 90^0

Таблиця 1.

Результати моделювання роботи алгоритму оцінювання під час розвороту на 90^0 для різних значень параметра γ.

Значення параметра γ.	Характер алгоритму	СКО максимальних помилок оцінювання по координатам X,Y,Z під час зміни траєкторії руху, м			Помилки по швидкостям, м/с		
		σX	σY	σZ	σVx	σVy	σVz
0	Нестійкий	-	-	-	-	-	-
0,1	Стійкий	19	6	7	18	6	0,1
0,4	Стійкий	9	1,7	1,5	12	5	0,1
0,8	Стійкий	5,8	1,9	0,4	10	3	0,1

Результати моделювання роботи алгоритму показують, що при γ = 0 алгоритм нестійкий, помилки оцінювання по всім координатам швидко зростають, тобто відомий фільтр Калмана нестійкий. У той самий час при значеннях 0.4 ≤ γ ≤ 0.8 (табл. 1) запропонований алгоритм забезпечує стійкість процесу оцінювання.

Аналіз величини помилки оцінювання за координатами і швидкостями із усередненням по 100 реалізаціям показує, що з прямолінійного руху максимальна помилка за координатами становить 4,5 м при γ=0.1, а мінімальна 1.6 м при γ=0.8, але в ділянці маневру - максимальна помилка по координатам становить 18 м при γ=0.1, а мінімальна 5 м при γ=0.4. Також на ділянці маневру максимальна помилка за швидкостями становить 18 м/с при γ=0.1, а мінімальна - 10 м/с при γ=0.4.

Оптимальне значення з допомогою якого отримані такі помилки оцінювання дорівнює 0.8. При цьому значення забезпечується стійке оцінювання ПР БПЛА при досягненні мінімального значення помилки визначення ВС в середньому за 8 кроків оцінювання.

Однак, основним недоліком розглянутого алгоритму є той факт, що у разі наявності маневру, фільтр Калмана-Бьюсі деякий час працюватиме на перехідній ділянці оцінювання, а після чого на стаціонарному. У той же час, при короткочасному маневрі, робота фільтру Калмана-

Бьюсі завжди буде на перехідній ділянці. А якщо характер руху БПЛА є траєкторією руху об'єкта, що постійно маневрує, то за допомогою алгоритмів на основі фільтра Калмана отримання високоточних оцінок ПР неможливо.

І тим не менш, для високоточного визначення координат ПР БПЛА як елементів інфокомунікаційних сенсорних мереж можна застосовувати алгоритми на основі фільтра Калмана-Бьюсі або методу найменших квадратів (МНК). Потенційна точність оцінювання цих методів практично однакова. Оптимальним підходом до оцінювання ПР є використання цих методів одночасно. Причому в такій послідовності: спочатку МНК для одержання оцінки вимірювань, а далі фільтр Калман-Бьюсі для оцінки ПР. Іншими словами, такий фільтр необхідно використовувати за наявності відомої моделі руху. Але це тільки при роботі з БПЛА, що маневрує, у разі наявності постійного маневру такий підхід не прийнятний. Отже, для оцінювання ПР БПЛА, які постійно маневрують, необхідне використання методів оцінювання вибірки вимірювань.

Такий підхід дозволяє досить просто вирішити питання вибору моделі руху в умовах постійного маневру. При цьому питання забезпечення стійкості оцінювання - це наявність вибірки вимірювань, а забезпечення необхідної точності - підбір полінома апроксимації. Ще одним важливим параметром, величина якого визначає помилку оцінювання, є ширина "ковзного вікна". Цей параметр може задаватися у вигляді часового інтервалу або кількості вимірювань, за якими надалі визначаються коефіцієнти апроксимації та оцінка параметра, що знаходиться.

Завдання вибору ступеня полінома апроксимації залежить від виду та інтенсивності маневру БПЛА. Наприклад, вважається, що у польоті БПЛА здійснює перехід від рівномірного руху до маневру, то ступінь полінома слід підвищувати. І при цьому кількість членів апроксимуючого полінома збільшується. Змінюється як ступінь полінома, а й значення кожного коефіцієнта цього полінома. Зауважимо, що ступінь полінома змінюється дискретно залежно від помилки оцінювання.

Тому досліджуємо методом математичного моделювання наступне завдання: не збільшуючи ступеня апроксимуючого полінома забезпечити підвищення точності оцінювання при оцінці ПР БПЛА, що постійно маневрує.

Для цього розглянемо ряд П'юїзе [6] з однією змінною. Це формальний вираз алгебри:

$$F(x) = \sum_{n=n_o}^{\infty} a_n x^{\frac{n}{m}}, \qquad (12)$$

в якому число n_0 - ціле, число - натуральне число (при виходить звичайний статечний ряд), коефіцієнти a_n беруться з деякого кільця

Враховуючи той факт, що *F(x)* набуває речових значень, у разі коли n<m, коефіцієнти a_n повинні бути комплексними.

У деяких практичних програмах змінна *x* не може бути комплексною, наприклад, якщо така змінна *x* - час. Ряд (12) у разі коли змінна *x* набуває речового значення, а значення n_o = 0 може бути представлений у вигляді суми двох рядів (без залишкового члена:

$$F(x) = T(x) + R(x) \quad . \qquad (13)$$

Тут *T(x)* – ряд Тейлора, *R(x)* – ряд, що з дробових членів. Назвемо ряд (13) дробовим рядом Тейлора. Відомий ряд Тейлора [7] у цілих похідних має вигляд:

$$f(x) = f(x_0) + f(x_0)'(x-x_0) + f(x_0)'' \frac{(x-x_0)^2}{2!} + .. f(x_0)^n \frac{(x-x_0)^n}{n!} \qquad (14)$$

або у загальному вигляді $f(x) = \sum_{k=0}^{n} f(x_0)^k \frac{(x-x_0)^k}{k!}$, k = 0,1,2,3,… .

Уявим ряд Тейлора (14) для дробових похідних [6]. Для цього функції заданої на відрізку [a,b] можуть бути представлені у вигляді:

$$D_{a+}^{a} f(x) = \frac{1}{\Gamma(1-a)} \frac{d}{dx} \int_a^x \frac{f(x)dt}{(x-t)^a}, \qquad (15.а)$$

$$D_{b-}^{a} f(x) = \frac{1}{\Gamma(1-a)} \frac{d}{dx} \int_x^b \frac{f(x)dt}{(x-t)^a} \qquad (15.б)$$

і називаються правою і лівою похідними дробовими порядку , 0<*a*<1, відповідно лівосторонньої і правосторонньої. Тут *Г(1-a)* - гама функція Ейлера.

Дробові похідні у вигляді (13) ще називають [6] похідними Рімана - Ліувілля. У випадку, якщо є загальний аналітичний вираз для похідної *n*-го порядку, поняття дробової похідної може бути введене природним шляхом узагальнення даного виразу (коли це можливо) на випадок довільного числа .

Тоді загальновідомий запис першого похідного для функцій *f(x)* = x^k, представимо як:

$$\mathrm{f(x)}' = \frac{d}{dx}\,\mathrm{f}(x) = k\,x^{k-1}$$, а узагальнено:

$$\frac{d^n}{dx^n}\,x^k = \frac{k!}{(k-n)!}\,x^{k-n}, \qquad (16)$$

Після заміни факторіалів гамма-функціями можна подати у вигляді:

$$\frac{d^n}{dx^n}\,x^k = \frac{\Gamma(k)}{\Gamma(k-n+1)}\,x^{k-n}. \qquad (17)$$

Далі без суворого математичного обґрунтування введемо припущення: якщо існує ряд Тейлора для похідних, то такий ряд може існувати і з дробовими похідними для n_o = 0, і речовими коефіцієнтами.

Тоді з урахуванням існування [6] дробових похідних такий ряд має вигляд:

$$f(x_0) = \sum_{k=0}^{n} f(x_0)^k \;\; \frac{\Gamma(k)}{\Gamma(k-n+1)}\,(x-x_0)^{\,k-n}, \qquad (18)$$

де *k*=0, 0.5, 1, 1.5, 2, 2.5…

Назвемо додаткові члени введеного ряду дробовими. Зауважимо, що з ряду Тейлора (18) не можна стверджувати, що ряд є схожим як і ряд (12). Причиною цього є відсутність ортогональності членів одержаного ряду.

Так, наприклад, для ряду (12) функції 1, $x^{\,1}$, $x^{\,2}$,…. $x^{\,n}$ - є ортогональними, в той же час для ряду (16) $x^{\,1/2}$, $x^{\,1}$, $x^{\,3/2}$, $x^{\,2}$…. дробові та цілі члени є ортогональними в іншій метриці. Можна стверджувати, що ряд (18), має розширені властивості порівняно з рядом (14).

Зауважимо, що автори не претендують на математичну строгість використання ряду (16). Наше завдання: з'ясувати шляхом моделювання, що з використанням ряду Тейлора (16). для оцінювання ПР БПЛА, яке маневрує, методом МНК чи призведе лі до підвищення точності оцінювання порівняно з використанням ряду (12). Надія на цей виграш обумовлена тим, що використання ряду (16) дозволяє збільшити дискретність оцінки похідних складових траєкторії руху БПЛА.

Для початку порівняємо дробовий ряд Тейлора зі звичайним його поряд. Обмежимося також використанням ряду (18) для похідних не вище 3/2 і залишимо поки що осторонь фізичний зміст коефіцієнтів при дробових похідних да спробуємо пояснити з математичної точки зору сутність дробової похідної.

Наприклад, для похідної дробової дорівнює 1/2 її величина займає середнє значення між першоподібною і першою похідною. Відповідно, похідна 3/2 - середнє значення між першою та другою похідною і т.д. При цьому можна стверджувати, що якщо, наприклад, *n* - я похідна дорівнює 0, а n-1 відмінна від нуля, то похідна, яка займатиме проміжне положення не завжди буде нульовою. Проведений авторами попередній аналіз фізичного сенсу коефіцієнта апроксимації при ступені 3/2 показує, що його не потрібно враховувати, якщо значення цього параметра не використовується в наступних розрахунках у цьому і є деяке обмеження використання дробових рад Тейлора.

Тим більше, такі випадки існують при використанні МНК з ортогональними поліномами Чебишева [8], привабливість яких полягає в тому, що при підвищенні ступеня полінома необхідно розрахувати лише один коефіцієнт при цьому ступеню, а при зменшенні нічого не потрібно розраховувати - просто слід відкинути старший член ряду Чебишева. У цьому самі коефіцієнти низки фізичного сенсу немає, а за використанні ортогональних поліномів Чебишева необхідно додатково визначати відомі фізичні значення: становище, швидкість і прискорення. Виходячи з

вищевикладеного, проаналізуємо застосування введеного ряду Тейлора (16) з дробовими похідними стосовно задачі оцінювання ПР БПЛА.

Нижче наведено деякі результати моделювання, отримані за допомогою програми MATLAB. На рис. 3 показані результати апроксимації полінома четвертого ступеня з розподіленим шумом за нормальним законом (поліном імітації) з дисперсією помилки рівною 10 $м^2$. - штрих пунктирна лінія, на всьому інтервалі за МНК поліномом другого ступеня виду:

$$Y = a_0 + a_1 x^1 + a_2 x^2 \ , \tag{19}$$

- суцільна лінія, і за МНК поліномом ступеня 3/2 через дробові ступеня ½:

$$Y = a_0 + a_1^* x^{0.5} + a_2 x^1 + a_3^* x^{\frac{3}{2}} \ , \tag{20}$$

де a_1^* , a_3^* - коефіцієнти має сенс дробових похідних - пунктирна лінія.

З графіків видно, що помилка оцінювання при оцінюванні МНК поліномом (18) зменшується на 10-15%.

Аналогічно на рис 4. показаний результати апроксимації полінома третього ступеня з шумом розподіленим за нормальним законом з дисперсією помилки, що дорівнює 5 $м^2$ - штрих пунктирна лінія, за методом МНК поліномом (17) - суцільна лінія, і дробовим поліномом виду:

$$Y = a_0 + a_1 x^{0.5} + a_2 x^1 \quad . \tag{21}$$

Результати моделювання показують, що і в даному випадку застосування полінома з дрібним ступенем дозволяє підвищити точність оцінювання до 20%.

Ці та інші результати моделювання (графіки мають вигляд аналогічний на рис. 3,4) для наочності зведені в табл. 2.

З таблиці 2 видно, що використання запропонованого дробового ряду Тейлора в задачі оцінювання ПР постійно маневрують БПЛА, коли їх траєкторія руху описується поліномом більш високого ступеня, що дозволяє підвищити точність оцінювання. Понад те, кожного класу БПЛА можна зафіксувати ступінь полінома для оцінювання ПР. Це значно спростить структуру програмного забезпечення без погіршення точності.

Зауважимо, що оцінювання з МНК з використанням дробових рядів Тейлора переважно в тому випадку, коли порядок полінома імітації вище за поліном апроксимації. Якщо ступінь поліномів імітації і апроксимації збігаються, то використання дробових рядів Тейлора не має сенсу. Але саме тут і проявляється основна перевага використання дробового ряду Тейлора, яка полягає в тому, що знати порядок полінома апроксимації в загальному випадку не потрібно. Інакше кажучи, якщо є вимоги до точності оцінювання, слід заздалегідь вибрати ступінь дробового ряду Тейлора, що дозволить забезпечити підвищення точності оцінювання проти відомим рядом Тейлора.

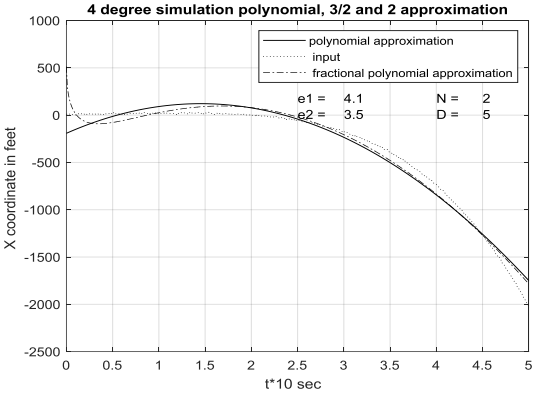
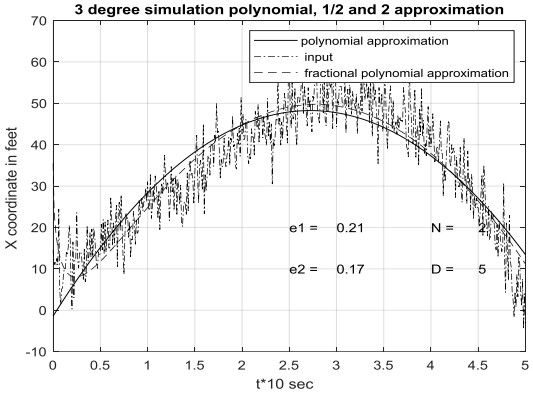


Рис 3. Апроксимація полінома четвертого ступеня дисперсією помилки, що дорівнює 10 $м^2$



Р Рис. 4. Апроксимація полінома третього ступеня з дисперсією помилки, що дорівнює 5 $м^2$

Таблиця 2.
Характеристики помилок оцінювання

Ступінь апроксимації поліномом імітації	4	3	3	3	3
Ступінь апроксимації цілим поліномом	2	2	2	2	3
Ступінь апроксимації дробовим поліномом	3/2	1/2	2	2.5	2.5
Помилка апроксимації цілим поліномом	4.1	0.21	0.33	0.21	0.026
Помилка апроксимації дробовим поліномом	3.5	0.17	0.26	0.02	0.031
Підвищення точності, %	15%	20%	22%	90%	-15%

Подальше дослідження полягало у порівнянні показників оцінювання МНК у "ковзному вікні" і з оцінкою поліномами Чебишева, дробовими і звичайними рядами Тейлора. Для такого порівняння розглянемо поліноми Чебишева першого, другого та третього роду, поліноми на основі дробового ряду Тейлора та поліноми на основі традиційного ряду Тейлора або просто алгебраїчні:

$$y(t) = a_o + a_1 t + a_1 t^2, \quad (22)$$

$$y(t) = a_o + a_1 t + a_1 t^2 + a_1 t^3, \quad (23)$$

багаточлени Чебишева першого роду другого і третього порядку:

$$T_o(x) = 1;\ T_1(t) = x;\ T_2(x) = 2x^2 - 1;\ T_3(x) = 4t^3 - 3x;$$

$$T_n(x) = 2x\, T_n(x) - T_{n-1}(x); \quad (24)$$

$$y(t) = a_o + a_1 t + a_2 (2t^2 - 1),$$

$$y(t) = a_o + a_1 t + a_2 (2t^2 - 1) + a_3 (4t^3 - 3x). \quad (25)$$

та дробові поліноми на основі ряду Тейлора:

$$y(t) = a_o + a_1 t^{0.5} + a_2 t^1. \quad (26)$$

$$y(t) = a_o + a_1 t^{0.5} + a_2 t + a_3 t^{1.5} \quad . \quad (27)$$

Припустимо, що БПЛА постійно здійснює маневр відповідно до полінома 3-го порядку та параметрів шуму розподіленого за нормальним законом розподілу нульовим середнім і дисперсією рівною 25 $м^2$. Поставимося також шириною "ковзного вікна" W=12 або 6, для многочленів Чебишева на інтервалі [-1;1].

Оцінювання МНК з будь-якими поліномами вимагає звернення матриці. При оцінюванні по МНК з поліномами Чебишева цьому інтервалі при великій ширині "ковзного вікна" виникають проблеми з зверненням матриці. У такому разі слід використовувати метод Зейделя. Відомо також, що багаточлени Чебишева мають найкраще наближення серед усіх відомих багаточленів.

При використанні багаточленів (25-26) також виникають проблеми із обігом матриці. Рекомендуємо використовувати інтервал оцінювання рівний [1;5] і тоді проблем із оберненням матриці не виникає.

Результати моделювання показані на рисунках 5,6 та табл. 3. Зокрема, на рис. 5,6 показані оцінки траєкторії руху алгебраїчним поліномом – штрих пунктирна лінія, поліномом Чебишева – пунктирна лінія, дробовим поліномом (26) – суцільна лінія, а в табл. 3 – характеристикі оцінювання.

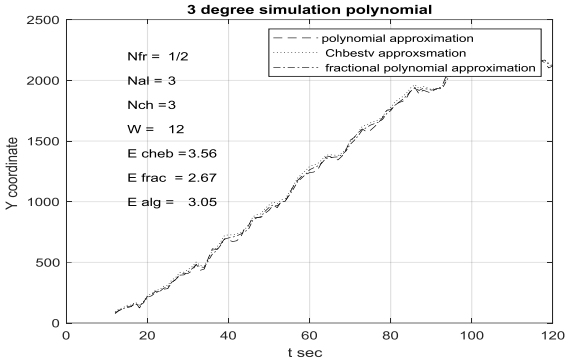


Рис. 5. Траєкторія руху зі ступенем дробового полінома Nfr = 1/2

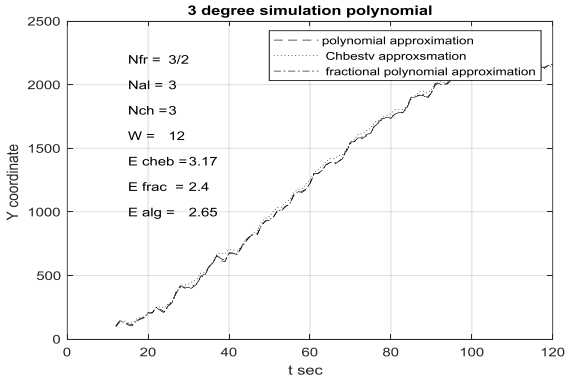


Рис. 6. Траєкторія руху зі ступенем дробового полінома Nfr = 3/2

Як видно з рис. 5 і табл. 3 точність оцінювання дробовим поліномом на 13% вище ніж алгебраїчним і на 25% вище ніж багаточлен Чебишева. Останнє обумовлено шириною інтервалу «ковзного вікна». У той же час, точності оцінювання дробовим і поліномом Чебишева збігаються. При варіанті моделювання на рис. 6 точність оцінювання дробовим поліномом на 8% вище ніж алгебраїчним і на 25% вище за поліном Чебишева, що обумовлено шириною «ковзного вікна».

Таблиця 3.
Характеристикі оцінювання в «ковзному вікні»

№	Ширина вікна (W)	Ступінь полінома та помилка оцінювання	Алгебраїчний поліном	Поліном Чебишева	Дробний поліном
1 (рис.5)	12	ступінь полінома	Nal = 3	Nch = 3	Nfr = 1/2
		помилка оцінювання	3.05	3.56	2.67
2 (рис. 6)	12	ступінь полінома	3	3	3/2
		помилка оцінювання	2,65	3.17	2.4
3	6	ступінь полінома	3	3	1/2
		помилка оцінювання	2,93	2,45	2,55
4	6	ступінь полінома	3	2	1/2
		помилка оцінювання	2,87	2,65	2,58
5	6	ступінь полінома	3	2	3/2
		помилка оцінювання	2,25	2,14	2,22
6	6	ступінь полінома	3	3	3/2
		помилка оцінювання	2,52	2,25	2,41

Максимальна точність оцінювання досягається поліномом (26) із шириною «ковзного вікна» *W* = 12. З результатів моделювання та таблиці 3 випливає, що необхідно звернути увагу на поліном (26). Використання цього полінома, за певних умов, забезпечує максимальну точність оцінювання проти поліномами Чебишева і поліномом з урахуванням ряду Тейлора.

Висновки

1. Для інфокомунікаційних сенсорних мереж на основі БПЛА запропоновано стійкий алгоритм оцінювання ПР літаючих об'єктів для випадків їх різкого маневрування шляхом багаторазових вимірювань відстаней між ними, формування вектору стану та КМО координат та подальшого уточнення координат та їх похідних за допомогою фільтра Калмана.

2. Для БПЛА, що постійно маневрує, результати досліджень показують, що застосування дробових рядів Тейлора дозволяє суттєво розширити клас завдань при використанні МНК у задачах оцінювання ПР літаючих об'єктів як елементів бездротових сенсорних мереж, зокрема,

не використовувати рекурентні алгоритми оцінювання з елементами адаптації шляхом зміни ступеня полінома.

3. З результатів моделювання слід, що для БПЛА, яке постійно маневрує, найбільш прийнятним поліномом оцінювання є МНК з дрібними ступенями 1/2 і, на наш погляд, необхідне подальше дослідження поліномів з дрібними ступенями вище ступеня 3/2.

4. Застосування дробових поліномів в інфокомунікаціях та інших галузях техніки обмежується відсутністю фізичного сенсу дробових похідних і проте проведене дослідження з використання дробових поліномів показало отримання більшої точності оцінювання ПР БПЛА порівняно з поліномами Чебишева за великої ширини «ковзного вікна».

Література

1. Romaniuk V. Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV / V. Romaniuk, O. Lysenko, A. Romaniuk and. Zhuk O. *Information and telecommunication scienc*es. 2020. Vol, №. 1. pp. 102-107.
2. Yakornov Y. and Tsukanov O. Sustainable Algorithm for Estimating the Motion Parameters of Unmanned Aerial Vehicles. International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) – Proceedings, September 2019, pp. 1-5.
3. Langdon M. ZigBee goes underground, E&T Magazine. 2009, Aug.
4. Grewal M. and Andrews A. Kalman Filtering — Theory and Practice Using MATLAB, Wiley.2001.
5. Мельник Н.О. Полная математическая модель беспилотного летательного аппарата в условиях движения с возмущающими воздействиями. *Вестник Воронежского государственного технического университета I*SSN: 1729-6501, 2015, том 11, № 2, С. 31-33.
6. Kilbas A., Srivastava H. and Trujillo J. Theory and Applications of Fractional Differential Equations. Amsterdam: Elsevier, 2006.
7. Sierociuk D. Fractional Kalman Filter algorithm for states, parameters and order of fractional system estimation, Int. J. Appl. Math. Comput. Sci., 2006, Vol.16, No.1, pp, 129–140.
8. Lysenko O., Novikov V. and Alekseeva I. Optimization of Unmanned Aerial Vehicle Path for Wireless Sensor Network Data Gathering. 3rd International Conference: Actual problems of unmanned aerial vehicles developments (APUAVD-2015) – Proceedings, October 2015, pp.280-283.

References

1. Romaniuk V. Increasing the efficiency of data gathering in clustered wireless sensor networks using UAV / V. Romaniuk, O. Lysenko, A. Romaniuk and. Zhuk O. *Information and telecommunication scienc*es. 2020. Vol, №. 1. pp. 102-107.
2. Yakornov Y. and Tsukanov O. Sustainable Algorithm for Estimating the Motion Parameters of Unmanned Aerial Vehicles, // International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) – Proceedings, September 2019, pp. 1-5.
3. Langdon M. ZigBee goes underground, E&T Magazine, 2009, Aug.
4. Grewal M. and Andrews A. Kalman Filtering — Theory and Practice Using MATLAB, Wiley, 2001.
5. Melnik N.O. Polnaia matematicheskaia model bespilotnogo letatelnogo apparata v usloviiakh gvizheniia s vozmushchaiushchimi vozdejstviiami. [Complete mathematical model of an unmanned aerial vehicle in traffic conditions with disturbing influences]. Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta ISSN: 1729-6501, 2015, tom 11, № 2, C. 31-33.
6. Kilbas A., Srivastava H. and Trujillo J. Theory and Applications of Fractional Differential Equations. Amsterdam: Elsevier, 2006.
7. Sierociuk D. Fractional Kalman Filter algorithm for states, parameters and order of fractional system estimation, Int. J. Appl. Math. Comput. Sci., 2006, Vol.16, No.1, pp, 129–140.
8. Lysenko O., Novikov V. and Alekseeva I. Optimization of Unmanned Aerial Vehicle Path for Wireless Sensor Network Data Gathering // 3rd International Conference: Actual problems of unmanned aerial vehicles developments (APUAVD-2015) – Proceedings, October 2015, pp.280-283.

УДК 944.577

АНАЛІЗ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ НЕГАТИВНОГО ЗВОРОТНЬОГО ЗВ'ЯЗКУ НА ЗМІННОМУ СТРУМІ ДЛЯ СТАБІЛІЗАЦІЇ ПАРАМЕТРІВ ТРАНЗИСТОРНИХ АНАЛОГІВ ІНДУКТИВНОСТІ

DOI 10 36994 / 2788- 5518- 2022-02-09

***Осадчук О.В.**, д.т.н., проф. Вінницький національний технічний університет, Вінниця, Україна. osadchuk.av69@gmail.com*

***Осадчук Я.О.**, к.т.н. Вінницький національний технічний університет,. Вінниця, Україна. e*osadchuk.j93@gmail.com

***Думенко Д.О.** Вінницький національний технічний університет, Вінниця, Україна. edoomdenny@gmail.com*

***Анотація:** у статті розглядається доцільності використання негативного зворотнього зв'язку на змінному струмі для стабілізації параметрів транзисторних аналогів індуктивності. Проаналізовано транзисторні каскади із спільним колектором та внесеною реактивністю між базою та колектором. Розглянуто вплив паралельного, послідовного та паралельно-послідовного зворотнього зв'язку на них. Проведені розрахунки залежностей активного, реактивного опору, індуктивності та добротності в функції глибини паралельного негативного зворотнього зв'язку(НЗЗ), наведені графіки залежностей еквівалентної індуктивності і добротності. Доведено ефективність стабілізації параметрів транзисторних аналогів індуктивності (при змінному та постійному струмі) при взаємодії таких дестабілізуючих факторів як нестабільність джерел живлення, зміну температури в діапазоні до +50° для германієвих та +70° для кремнієвих транзисторів. Наведена базова схема транзистора для проведення аналізу впливу паралельного НЗЗ, на основі якої виведена спрощена еквівалентна схема з врахуванням впливу опору зворотнього зв'язку, а також розрахункова схема, отримана переутворюючи трикутник в еквівалентну зірку. Використовуючи метод контурних струмів і виконуючи неважкі перетворення отримані вирази для визначення вхідного активного та реактивного опорів, індуктивності, добротності окремих схем та узагальнених випадків.*

Доведено, що температурна стабільність значно покращується при заміні постійних опорів температурно-чуттєвими елементами. Наведено одну із схем транзисторних аналогів індуктивності із використанням термочутливого елементу в колі живлення.

***Ключові слова:** зворотній зв'язок, транзисторний аналог індуктивності, еквівалентна схема, сигнал, струм, контур, вплив, стабілізація.*

ANALYSIS OF THE EXPEDIENCY OF USING NEGATIVE FEEDBACK ON ALTERNATING CURRENT FOR STABILIZATION OF TRANSISTOR ANALOGS OF INDUCTANCE PARAMETERS

***Oleksandr Osadchuk,** Dr.habil., Prof. Vinnytsia National Technical University, Vinnytsia, Ukraine. : osadchuk.av69@gmail.com*

***Iaroslav Osadchuk,** Ph.D. Vinnytsia National Technical University, Vinnytsia, Ukraine. osadchuk.j93@gmail.com*

***Denys Dumenko.** Vinnytsia National Technical University, Vinnytsia, Ukraine. doomdenny@gmail.com*

***Abstract:** the article exa*mines the expediency of using negative feedback on an alternating current to stabilize the parameters of transistor analogs of inductance. Transistor cascades with a common collector and introduced reactivity between the base and the collector are analyzed. The influence of parallel, serial and parallel-serial feedback on them is considered. Calculations of the dependences of active resistance, reactive resistance, inductance, and Q-factor as a function of the depth of parallel negative feedback are made, graphs of the dependences of equivalent inductance and Q-factor are given. The effectiveness of stabilizing the parameters of transistor analogs of inductance (at alternating and direct current) in the interaction of such destabilizing factors as instability of power sources, temperature changes in the range of up to +50° for germanium and +70° for silicon transistors has been proven. The basic diagram of a transistor for analyzing the effect of a parallel negative feedback is presented, based on which a simplified equivalent circuit is derived taking into account the influence of feedback resistance, as well as a calculation scheme obtained by *transforming a triangle into an equivalent star. Using the method of loop currents and performing easy transformations, expressions are obtained for*

determining the input active and reactive resistances, inductance, Q factor of individual circuits and generalized cases.

It has been proven that temperature stability is significantly improved when constant resistances are replaced by temperature-sensitive elements. One of the circuits of transistor analogues of inductance using a thermosensitive element in the power supply circuit is given.

Key words: *feedback, transistor analogue of inductance, equivalent circuit, signal, current, circuit, influence, stabilization.*

Вступ

Одним з найголовніших методів стабілізації параметрів транзисторних структур індуктивності є внесення каскад зворотнього зв'язку в систему. Таким чином, відбувається компенсація нестабільності вихідного сигналу, шляхом передачі його частини на вхід оброблюючого пристрою.

Вибір каскаду зворотнього зв'язку залежить від бажаного результату, та необхідного рівня сигналу. Так, застосувавши одні рішення, можна можна отримати високо стабільний сигнал, проте невеликої амплітуди, що буде потребувати внесення додаткового підсилювального каскаду. І навпаки, можна досягти ще більший коефіцієнт підсилення каскаду, але підвищено чутливий до чинників впливу.

В статті приведено аналіз доцільності використання основних видів зворотніх зв'язків на змінному струмі для стабілізації параметрів ТАІ(транзисторних аналогів індуктивності). Будемо розглядати каскади з спільним колектором із позитивною реактивністю між колектором і базою, охоплені паралельним, послідовним та паралельно-послідовним зворотнім зв'язком.

Розглядаючи стабілізуючу дію робочого режиму на параметри ТАІ[1] необхідно обов'язково приділити увагу аналізу доцільності використання основних видів зворотніх зв'язків на змінному струмі для стабілізації параметрів ТАІ. Будемо розглядати каскади з спільним колектором із позитивною реактивністю між колектором і базою, охоплені паралельним, послідовним та паралельно-послідовним зворотнім зв'язком.

При визначенні впливу зворотнього зв'язку на параметри ТАІ будемо використовувати спрощені еквівалентні схеми[2], тому аналіз буде нести більш якісний характер, окрім того будемо розглядати випадки, коли параметри ТАІ визначаються опором зворотнього зв'язку та навантаження. Для спрощення аналізу будемо вважати, що опір в колах негативного зворотнього зв'язку (НЗЗ) є активним. Розглянемо кожну з видів НЗЗ окремо.

А) ТАІ з паралельним НЗЗ.

Каскад із паралельним НЗЗ наведено на рис. 1

Для проведення аналізу впливу паралельного НЗЗ представимо транзистор в схемі на рис. 1 у вигляді спрощеної еквівалентної схеми з врахуванням впливу $R''_{зз}$ (рис. 2)[3]. Переутворюючи трикутник утворений опорами $Z_е$, $Z_б$ та $R''_{зз}$ в еквівалентну зірку, отримаємо розрахункову схему рис. 3. :

$$\text{де} \quad R_1 = \frac{Z_е R''_{зз}}{R''_{зз} + Z_е + Z_б}, \qquad R_2 = \frac{Z_е Z_б}{R''_{зз} + Z_е + Z_б}, \qquad R_3 = \frac{R''_{зз} Z_б}{R''_{зз} + Z_е + Z_б}, \tag{1}$$

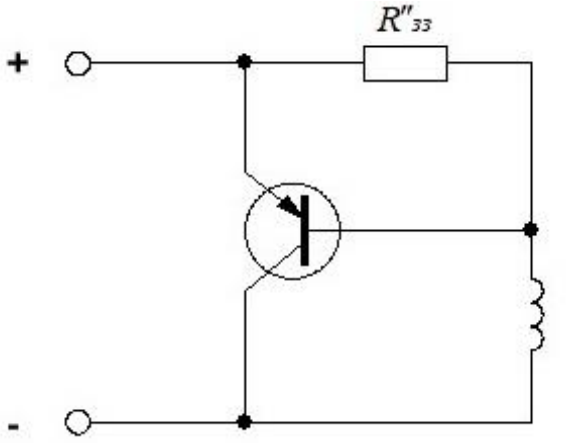


Рис. 1. Базова схема транзистора для проведення аналізу впливу паралельного НЗЗ

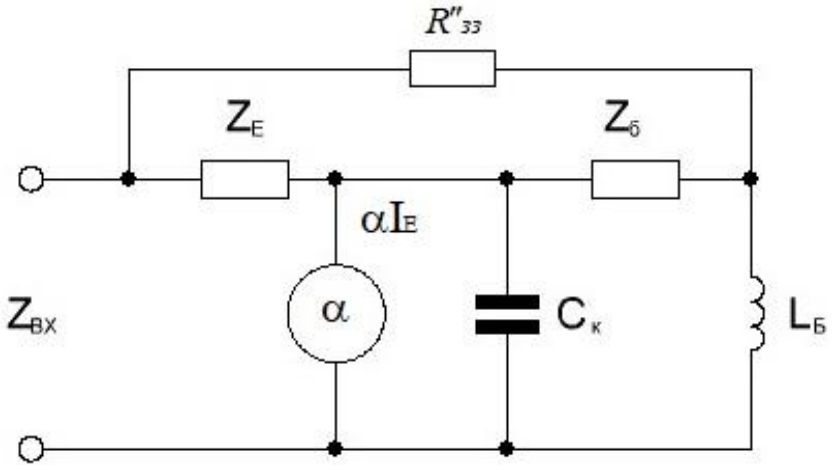


Рис. 2.Спрощена еквівалентна схема з врахуванням впливу $R''_{зз}$

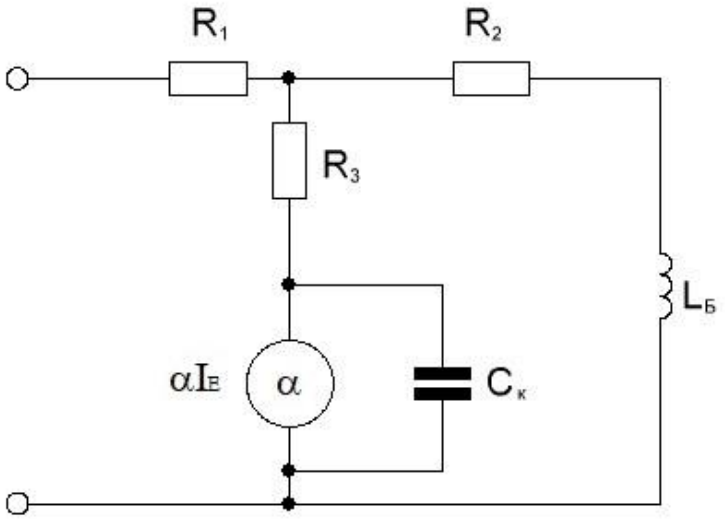


Рис. 3. Розрахункова схема, отримана переутворюючи трикутник в еквівалентну зірку

Застосовуючи метод контурних струмів для рис. 2 з врахуванням, що $I_e = I$, отримаємо

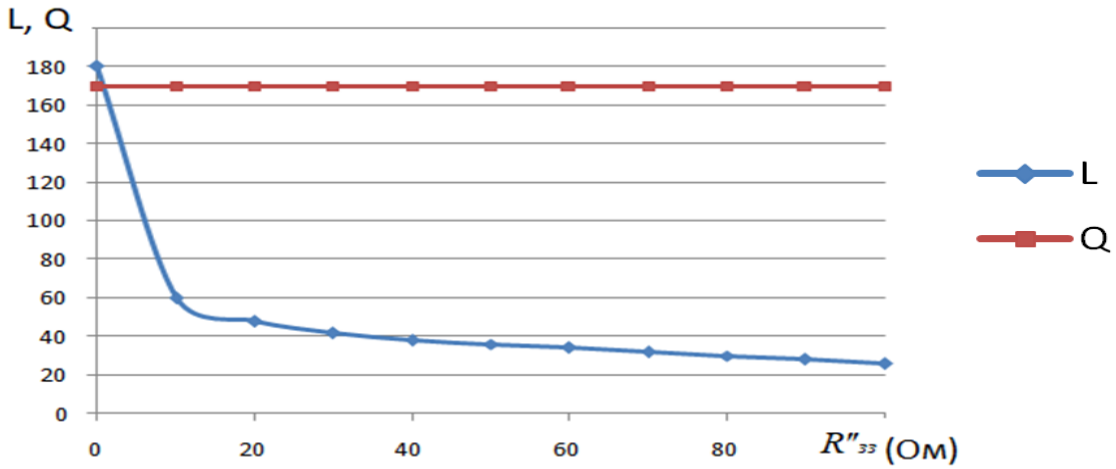


Рис. 4. Графіки залежностей еквівалентної індуктивності і добротності в функції глибини негативного зворотнього зв'язку

$$U_{вх} = I_1\left(R_1 + R_3 + j\omega L_б\right) - I_2\left(j\omega L_б - R_3\right)\ , \tag{2}$$

$$U = I_2\left(R_3 + R_2 + j\omega L_б + \frac{1}{j\omega C_к}\right) - I_1\left(R_3 + j\omega L_б - \alpha\frac{1}{j\omega C_к}\right)\ , \tag{3}$$

Виходячи з (3) визначимо I_2:

$$I_2 = \frac{I_1\left(R_3 + j\omega L_б - \dfrac{\alpha}{j\omega C_к}\right)}{\left(R_3 + R_2 + j\omega L_б - j\dfrac{1}{\omega C_к}\right)}\ , \tag{4}$$

$$Z_{вх} = \frac{U_{вх}}{I_1} = R_1 + R_3 + j\omega L_б - R_3 + \frac{j\left(\omega L_б + \dfrac{\alpha}{\omega C_к}\right)}{R_1 + R_3 + j\left(\omega L_б - \dfrac{1}{\omega C_к}\right)}\ , \tag{5}$$

Виконавши необхідні перетворення и розділивши дійсні та уявні частини отримаємо вираз для визначення еквівалентного активного та реактивного опорів, індуктивності та добротності:

$$R = \frac{A_1P + KA_2}{P^2 + K^2}, \tag{6}$$

$$X = \frac{A_2P - A_1K}{P^2 + K^2}, \tag{7}$$

$$L = \frac{A_2P - A_1K}{\omega\left(P^2 + K^2\right)}, \tag{8}$$

$$Q = \frac{A_2P - A_1K}{A_1P - A_2K}, \tag{9}$$

де $A_1 = NP + \omega L_б\left(e - k\right) + R_3^2$; $A_2 = NK - R_3e + \omega L_б\left(p - R_3\right)$;

$A_3 = R''_{ЗЗ} + Zб + Ze$; $N = R_1 + R_3$; $P = R_3 + R_2$..

На основі виразів (6 - 9) були проведені розрахунки залежностей R, X, L, Q в функції глибини паралельного негативного зворотнього зв'язку.

Графіки залежностей еквівалентної індуктивності і добротності в функції глибини негативного зворотнього зв'язку представлені на рис. 4. Як видно з рисунків збільшення глибини НЗЗ призводить до зменшення добротності, а індуктивність практично не змінюється. А відповідно паралельний НЗЗ може бути використаний для стабілізації добротності, при чому опір НЗЗ має незначну величину.

В) Каскад з послідовним зворотнім зв'язком по змінному струмі і спрощена еквівалентна схема для розрахунку зображена на рис. 5 та рис. 6 відповідно.

Використовуючи метод контурних струмів і виконуючи неважкі перетворення отримаємо вираз для визначення вхідного активного та реактивного опорів, індуктивності, добротності:

$$R = \frac{\left(Z_б + R_{ЗЗ}\right)\left[\left(Z_б + R_{ЗЗ}\right)m - \delta\right] + K\left(\tau - \omega L_б R_{ЗЗ}\right)}{\left(Z_б + R_{ЗЗ}\right)^2 + K^2}\ , \tag{10}$$

$$X = \frac{\left(Z_б + R_{ЗЗ}\right) + \left[\tau + \omega L_б\left(R_{ЗЗ} + 2Z_б\right)\right] - K\left[\left(Z_б + R_{ЗЗ}\right)m - \delta\right]}{\left(Z_б + R_{ЗЗ}\right)^2 + K^2}\ , \tag{11}$$

$$L = \frac{X}{\omega}, \qquad Q = \frac{X}{R},$$

де $K = \omega L_б - \dfrac{1}{\omega C_к}$; $m = Z_б - Z_e$; $l = \omega L_б + \dfrac{1}{\omega C_к}$;

$$\delta = \omega L_б \left(K + e\right) - Z_б{}^2; \qquad \tau = \mathrm{K}m + Z_б e;$$

На рис. 7 представлені графіки залежностей L, Q в функції глибини послідовного негативного зворотнього зв’язку при змінному струмі.

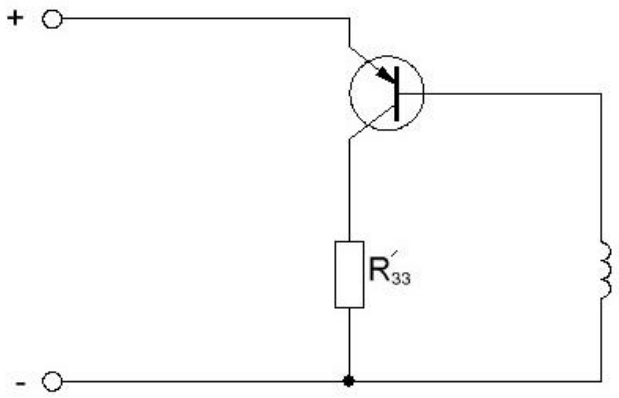


Рис. 5. Каскад з послідовним зворотнім зв’язком по змінному струмі

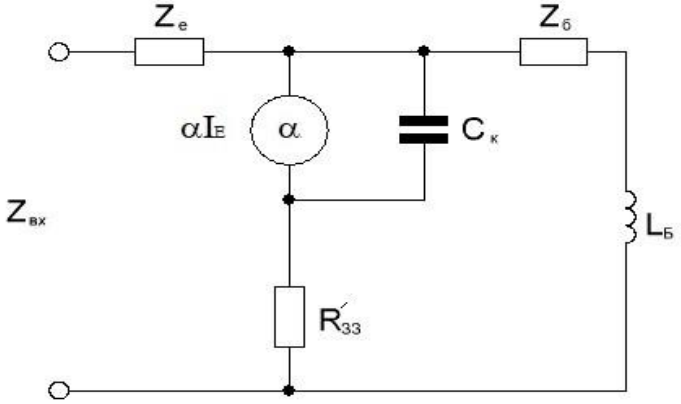


Рис. 6. Спрощена еквівалентна схема для розрахунку

Як видно з рисунку – послідовний НЗЗ здійснює стабілізуючу дію на індуктивність, добротність, проте остання різко зменшується при введені послідовного опору в коло колектора.[4]

С) Каскад із паралельно-послідовним НЗЗ.

Каскад із паралельно-послідовним НЗЗ при постійному струмі, та його спрощена еквівалентна схема для розрахунку зображені на рис. 8, 9.

На розрахунковій схемі рис. 9 значення опорів R_1, R_2, R_3; визначаються на основі формул (1).

Використовуючи метод контурних струмів [5]проведемо розрахунок вхідного опору, індуктивності та добротності схеми рис. 9.

Вирази для визначення цих величин мають вигляд:

$$L = \frac{BA - KM}{\omega\left(B^2 + K^2\right)}, \qquad Q = \frac{BA - KM}{MB + KA}, \tag{12}$$

Де $M = NB - \omega L_б\left(k + l\right) - R_3{}^2;$

$A = \omega L_б\left(B + R_3\right) + KN + lR_3;$

$B = R_2 + R_3 + R'_{ЗЗ};$ $N = R_1 + R_3;$.

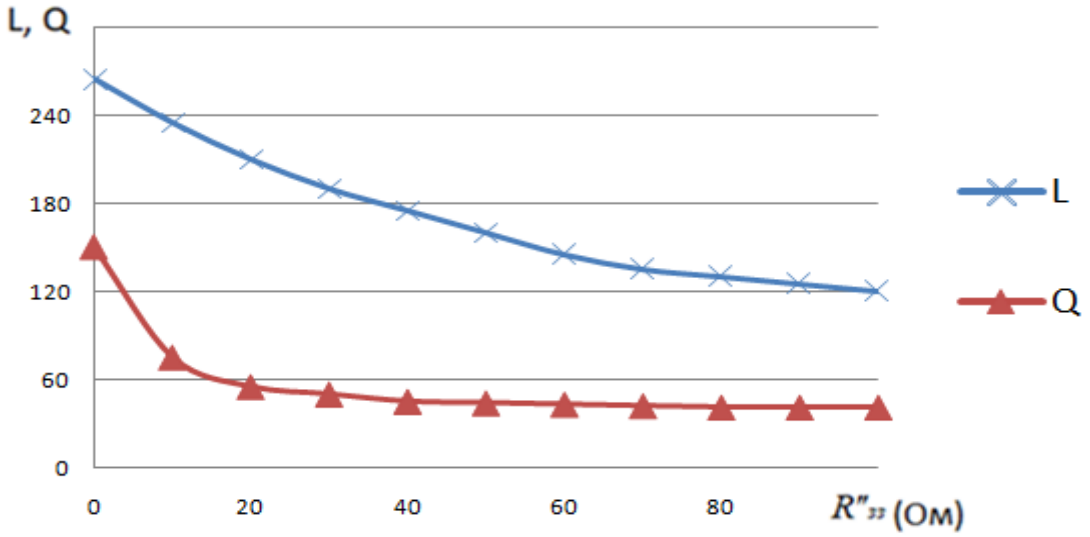


Рис. 7 .Гграфіки залежностей L, Q в функції глибини послідовного негативного зворотнього зв'язку при змінному струм.

Графіки залежності $L_{екв}, Q_{екв}$ в функції глибини послідовного $R'_{ЗЗ};$ та паралельного НЗЗ представлені на рис. 10 при змінному та постійному струмі дозволяє стабілізувати параметри транзисторних аналогів індуктивності при взаємодії таких дестабілізуючих факторів як нестабільність джерел живлення, зміну температури в діапазоні до +50° для германієвих та +70° для Si – транзисторів[6]. Проте при зміні температури в більш широкому діапазоні, тобто перехід в негативні області потребує прийняття додаткових заходів.

Температурна стабільність значно покращується при заміні постійних опорів температурно-чуттєвими елементами[7]. Одна із схем ТАІ з використанням термочутливого елементу в колі живлення представлена на рис. 11. Характеристика такого елемента підбирається експериментальним шляхом. З цією метою постійний опір в колі зворотнього зв'язку замінюється змінним, та змінюється температура відбиваючого середовища в межах ± С[8]. Для кожного значення температури підбирається величина опору, при якій величина добротності та індуктивності залишається постійною[9]. В результаті виходить необхідна характеристика термокомпенсуючого елемента.

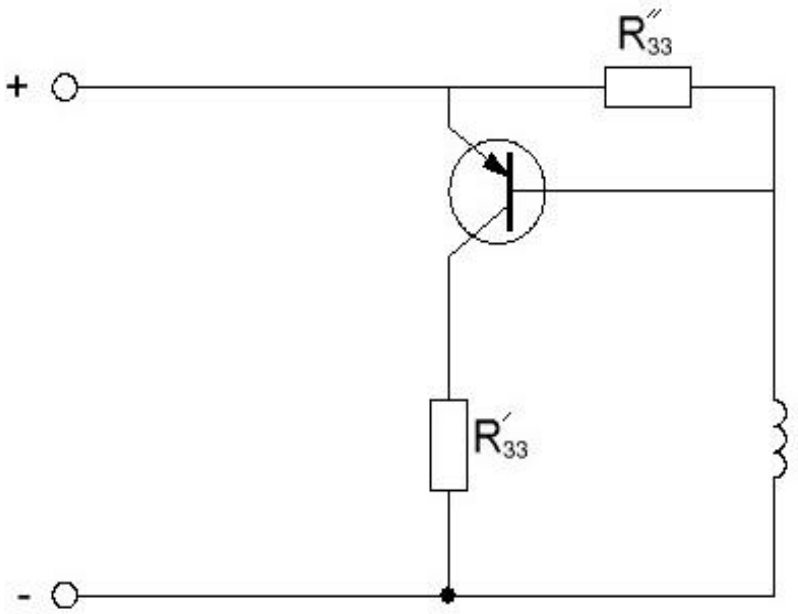


Рис. 8. Каскад із паралельно-послідовним НЗЗ при постійному струмі

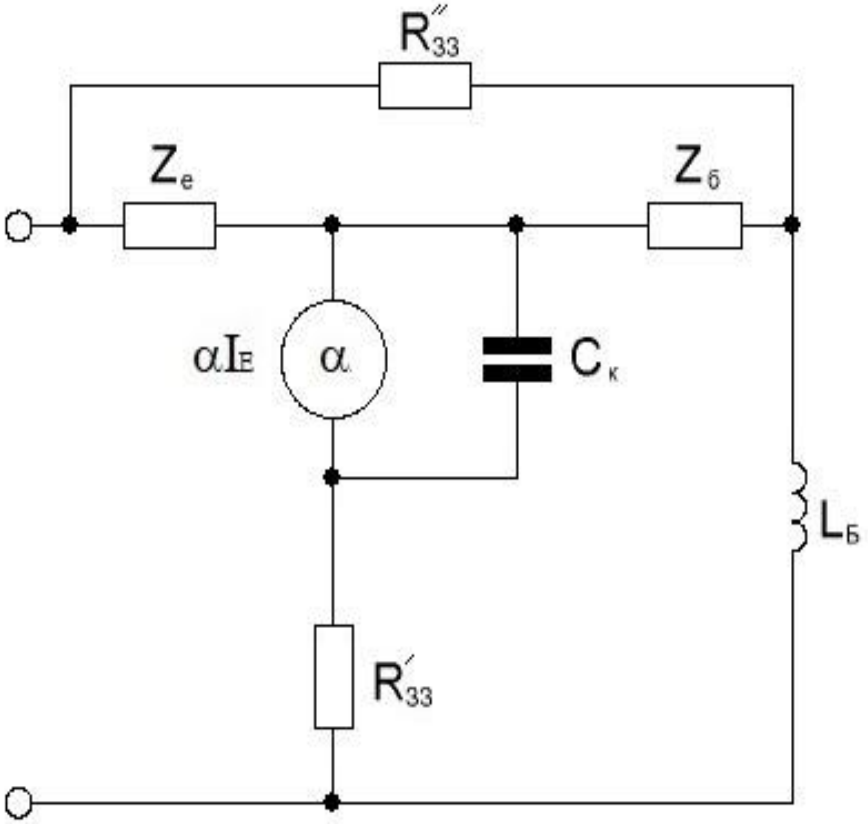


Рис. 9 . Розрахункова спрощена еквівалентна схема каскаду із паралельно-послідовним НЗЗ при постійному струмі

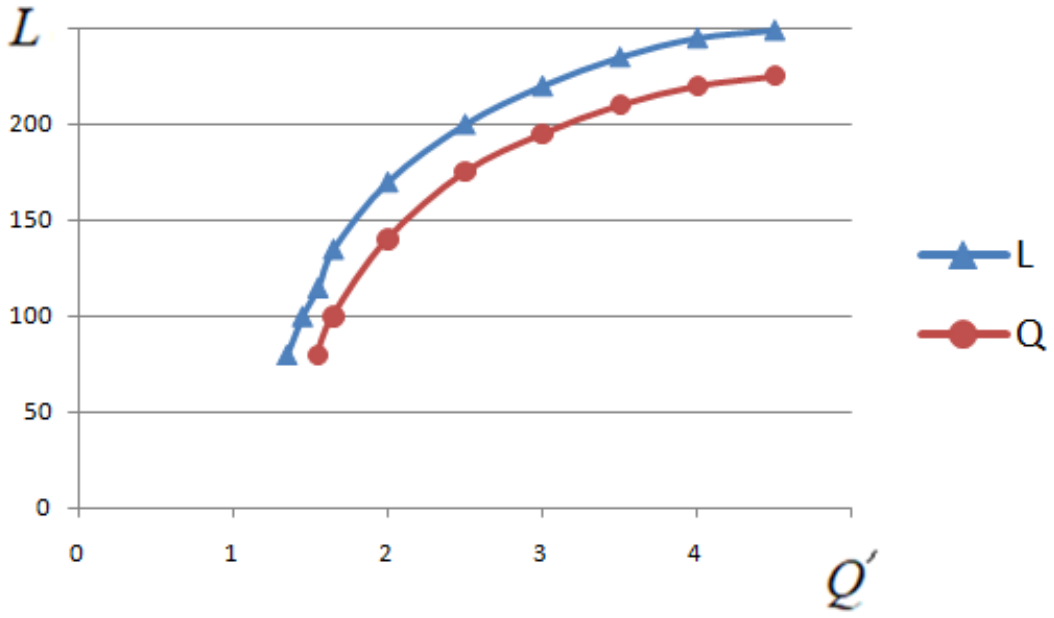


Рис. 10. Графіки залежності $L_{екв}, Q_{екв}$ в функції глибини послідовного $R'_{ЗЗ}$; та паралельного НЗЗ

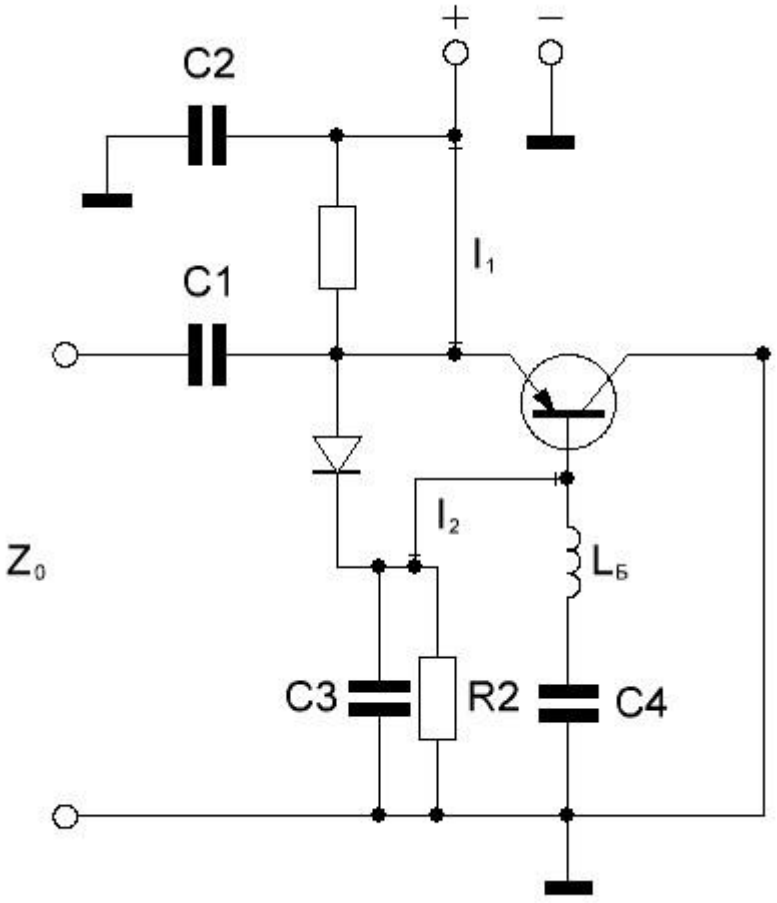


Рис. 11. Схема ТАІ з використанням термочуттєвого елементу в колі живлення

Висновки

1. Аналізуючи отримані результати - бачимо, що послідовний НЗЗ здійснює стабілізуючу дію на індуктивність, добротність, проте остання різко зменшується при введені послідовного опору в коло колектора.

2. Залежність індуктивності та добротності в функції глибини послідовного зворотнього зв’язку та паралельного негативного зворотнього зв’язку при змінному та постійному струмі дозволяє стабілізувати параметри транзисторних аналогів індуктивності при взаємодії таких дестабілізуючих факторів як нестабільність джерел живлення, зміну температури в діапазоні до +50° для германієвих та +70° для Si – транзисторів, однак, при зміні температури в більш широкому діапазоні, тобто перехід в негативні області потребує прийняття додаткових заходів.

Література

1. Ромашко В. Я., Батрак Л. М. Теорія електричних кіл-2. Нелінійні електричні кола : навч. посіб. Київ: КПІ імені Ігоря Сікорського, 2020. 88 с.
2. Осадчук В. С., Осадчук О. В., Семенов А. О. Генератори електричних коливань на основі транзисторних структур з від’ємним опором. Вінниця : УНІВЕРСУМ-Вінниця, 2009. 183 с.
3. Філинюк М. А., Войцеховська О. В.. Елементи та пристрої автоматики на основі нелінійних властивостей динамічних негатронів. Вінниця : УНІВЕРСУМ-Вінниця, 2008. 189 с.
4. Осадчук В. С., Осадчук О. В., Семенов А О. Функціональні вузли радіовимірювальних приладів на основі реактивних властивостей транзисторних структур з від’ємним опором та ін. Вінниця : ВНТУ, 2011. 336 с.
5. В. І. Сенько, М. В. Панасенко, Є. В. Сенько та ін Електроніка і мікросхемотехніка : Підручник у т4. Т. 1. Аналогові та імпульсні пристрої /.] – Харків: Фоліо, 2002. – 510 с.
6. O. Faruqe, M.T. Amin, Active Inductor with Feedback Resistor Based Voltage Controlled Oscillator Design for Wireless Applications / INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2018, PP. 57-64
7. Осадчук О. В., Семенов А. О. Математичне моделювання генератора НВЧ на основі транзисторної структури з від’ємним опором : Вісник Хмельницького національного університету. 2005. № 4, Ч. 1, Т. 2. – С. 256–259.
8. Філинюк М. А. Основи негатроніки. Том І. Теоретичні і фізичні основи негатроніки. Вінниця : УНІВЕРСУМ-Вінниця, 2006. 456 с.
9. S. Diao, Y. Wang, C. Wang VCO Design for Low-Power, High-Efficiency Transmitter Applications, in 2014 IEEE International Symposium on Radio-Frequency Integration Technology, Hefei, China, 2014, pp. 1-4.

References

1. Romashko V. Ya., Batrak L. M. *Teoriia elektrychnykh kil-2. Neliniini elektrychni kola : navch. posib.[Theory of electrical circuits-2. Nonlinear electrical circuits: a tutorial.]* Kyiv – KPI imeni Ihoria Sikorskoho, 2020. – 88 s. [in Ukrainian].
2. Osadchuk V. S., Osadchuk O. V., Semenov A. O. *Heneratory elektrychnykh kolyvan na osnovi tranzystornykh struktur z vid’iemnym oporom : monohrafiia [Generators of electrical oscillations based on transistor structures with negative resistance: monograph.* Vinnytsia : UNIVERSUM-Vinnytsia, 2009. – 183 s. [in Ukrainian].
3. Filyniuk M. A., Voitsekhovska O. V. *Elementy ta prystroi avtomatyky na osnovi neliniinykh vlastyvostei dynamichnykh nehatroniv : monohrafiia [Elements and devices of automation based on the nonlinear properties of dynamic negatrons: monograph]* .Vinnytsia : UNIVERSUM-
/ Vinnytsia, 2008. – 189 s. [in Ukrainian].
4. Osadchuk V. S., Osadchuk O. V., Semenov A O. *Funktsionalni vuzly radiovymiriuvalnykh pryladiv na osnovi reaktyvnykh vlastyvostei tranzystornykh struktur z vid’iemnym oporom : monohrafiia [Functional nodes of radio measuring instruments based on the reactive properties of transistor structures with negative resistance: monograph]* . Vinnytsia : VNTU, 2011. — 336 s. [in Ukrainian].
5. *Elektronika i mikroskhemotekhnika : Pidruchnyk u t4. T. 1. Analohovi ta impulsni prystroi [Electronics and microcircuitry: A textbook on v4. V. 1. Analog and pulse devices]* / [ta in.] / Kharkiv: Folio, 2002. – 510 s. [in Ukrainian].
6. O. Faruqe, M.T. Amin, Active Inductor with Feedback Resistor Based Voltage Controlled Oscillator Design for Wireless Applications / INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2018, PP. 57-64 [in English].
7. Osadchuk O. V., Semenov A. O. Matematychne modeliuvannia heneratora NVCh na osnovi tranzystornoi struktury z vid’iemnym oporom : [Mathematical modeling of a microwave generator based on a transistor structure with negative resistance] *Visnyk Khmelnytskoho natsionalnoho universytetu – Bulletin of the Khmelnytskyi National University.* – 2005. – № 4, Ch. 1, T. 2. – S. 256–259. [in Ukrainian].
8. Filyniuk M. A. *Osnovy nehatroniky. Tom I. Teoretychni i fizychni osnovy nehatroniky : monohrafiia [Fundamentals of negatonics]. Volume I. Theoretical and physical foundations of negatronics: monograph]* – Vinnytsia : UNIVERSUM-Vinnytsia, 2006. 456 s. [in Ukrainian].
9. S. Diao, Y. Wang, C. Wang VCO Design for Low-Power, High-Efficiency Transmitter Applications, *in 2014 IEEE International Symposium on Radio-Frequency Integration Technology*, Hefei, China, 2014, pp. 1-4. [in English].

УДК 621.391

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО ЗМЕНШЕННЯ РІВНЯ МІЖКАНАЛЬНИХ ЗАВАД В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ НА БАЗІ СИГНАЛУ OFDM

DOI 10 36994 / 2788- 5518- 2022-02-10

Полонський К. І. *Державний університет телекомунікацій, Київ, Україна.*
k.polonskiy26@gmail.com
Говорун О. І. *Державний університет телекомунікацій, Київ, Україна.*
govorun70@ukr.net

Анотація: *В роботі розглянуті питання підвищення ефективності функціонування телекомунікаційних систем передачі даних на базі технології паралельної передачі даних і частотного розподілу з мультиплексуванням фазомодульованого сигналу – технології OFDM (Orthogonal Frequency-Division Multiplexing). А саме: проведено аналіз структури сигналу OFDM; визначено, що зміна положення та параметрів піднесучої з складу даного OFDM-символу створюють міжканальну заваду, яка характеризується величиною потужності та залежить від кількості піднесучих в структурі даного OFDM-символу; подано перелік параметрів сигналу OFDM, які можуть впливати на появу міжканальних завад.*

На основі отриманих результатів запропоновано методологічний підхід до зменшення рівня міжканальних завад телекомунікаційних системах передачі даних на базі сигналу OFDM, визначено критерій оцінки ефективності і алгоритм реалізації поданої методології.

Ключові слова: сигнал OFDM, піднесуча, міжканальна завада, потужність міжканальної завади.

METHODOLOGICAL APPROACH TO REDUCING THE LEVEL OF INTERCHANNEL INTERFERENCE IN TELECOMMUNICATION SYSTEMS OF DATA TRANSMISSION BASED ON THE OFDM SIGNAL

Konstiantin Polonskyi. *State University of Telecommunications, Kyiv, Ukraine.*
k.polonskiy26@gmail.com
Oleg Govorun. *State University of Telecommunications, Kyiv, Ukraine.*govorun70@ukr.net

Abstract: *The article considers the power to improve the efficiency of the functioning of telecommunication data transmission systems based on the technology of parallel data transmission and the frequency division of the phase-modulated signal multiplexing - OFDM technology (Orthogonal Frequency-Division Multiplexing). OFDM technology today is considered as one of the most promising for encouraging wide-range digital radio communication systems over rich communication channels, OFDM technology may have a number of advantages, until such a high level of data transmission security, the possibility of influx on the signal / noise ratio, as a result, the independence of the influx of external factories, simple algorithms for processing data packets on the basis of the real algorithm of the simple Furious transformation . One hour before such a technology is short, there is a high sensitivity to the shift in frequency and phase of the input signal of the externally reference signal, low energy efficiency, staleness due to the Doppler effect when the technology is blocked in mobile devices.*

In the article, an analysis of the structure of the OFDM signal was carried out, and it was identified as one of the factors that can affect the efficiency of data transmission - the position and parameters of the skin subsystem in the warehouse of a given OFDM symbol.It is shown that changing the position of the parametr_in the bottom line from the warehouse of this OFDM-symbol creates an influx of one bottom line on the line - it is formed as a negative phenomenon, it is designated as an interchannel shift. The methodological approach was approved before changing the level of inter-channel factories of telecommunication systems for data transmission based on the OFDM signal.

Key words*: OFDM signal, subcarrier, inter-channel interference, inter-channel interference power.*

Вступ

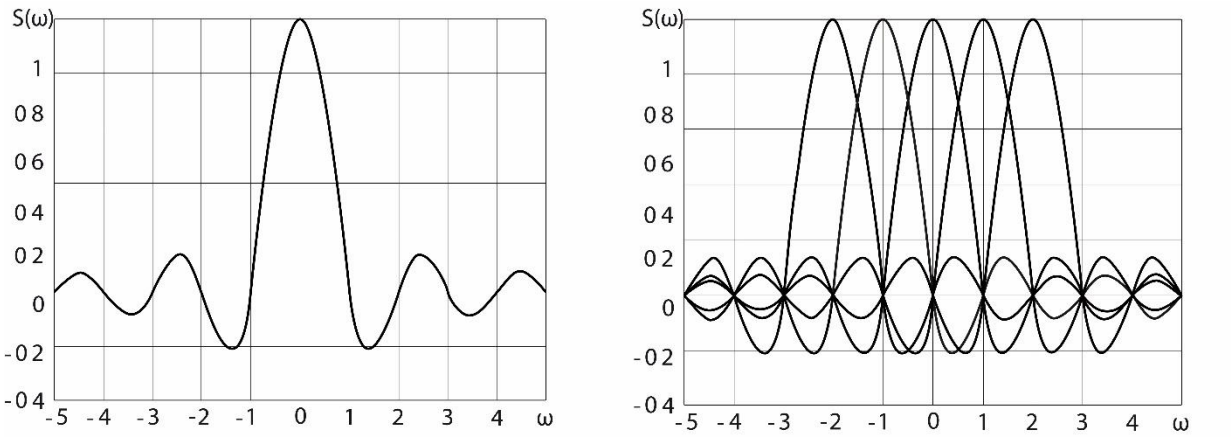
На сьогодення в найбільш сучасних та ефективних телекомунікаційних дротових та бездротових системах використовуються стандарти передачі даних, засновані на технології паралельної передачі даних і частотного розподілу з мультиплексуванням фазомодульованого сигналу – технології OFDM (Orthogonal Frequency-Division Multiplexing).

Технологія OFDM – одночасна передача потоку цифрових даних по багатьом частотним каналам (з багатьма несучими коливаннями) на сьогодні розглядається як одна з найбільш перспективних для побудови широкосмугових систем цифрового радіозв'язку по багатопроменевих каналах, що забезпечує досить високу спектральну ефективність цих систем. Однією із привабливих властивостей даної технології вважається відносно висока стійкість стосовно частотно-селективних завмирань і вузькосмугових завад [1].

Це пояснюється тим, що у системах з одним несучим коливанням, завмирання на даній частоті або вузькосмугова завада, що попадає на цю частоту, можуть повністю перервати передавання даних. У багаточастотних системах в аналогічних умовах виявляються подавленими лише незначна частина несучих коливань. А завадостійке кодування може забезпечити відновлення даних, загублених на подавлених несучих.

При OFDM високошвидкісний потік даних розбивається на велике число низько швидкісних потоків, кожний з яких передається у своєму частотному каналі (на своїй несучій частоті, інше визначення - піднесуча). Тобто в частотних каналах тривалість канальних символів може бути обрана досить велика, що значно перевищує час збільшення затримки сигналу в каналі. Отже, в кожному частотному каналі вражається лише незначна частина канального символу, яку можна вилучити з наступної обробки в приймачі за рахунок введення часового захисного інтервалу між сусідніми канальними символами при контрольованому зниженні швидкості передачі даних [1,2].

На рис 1. представлено графіки спектрів одного радіоімпульсу із прямокутною обвідною несучої у вигляді гармонійного коливання із частотою f_0 і одного OFDM - символу, що містить аналогічні радіоімпульси на декількох несучих, які відстоять по частоті один від одного на інтервалах кратно $\Delta f = 1/T$ [2,3].



А Б

Рис.1. Спектральна щільність одного елементарного символу (А)
і одного OFDM-символу (Б)

Технологія OFDM має ряд переваг, до яких слід віднести високу швидкість передачі даних, можливість впливу на співвідношення сигнал/шум та, як наслідок відносна незалежність від впливу зовнішніх завад прості алгоритми обробки пакетів даних на основі алгоритмів швидкого перетворення Фур’є та простота апаратної реалізації при можливості забезпечення одночасної передачі сигналів різного спектру через одну мережу. До переваг також можна віднести можливість застосування різних схем модуляції для кожної під несучої, що дозволяє адаптивно варіювати завадостійкість і швидкість передачі інформації [3,4].

Одночасно до недоліків такої технології слід віднести високу чутливість до зміщення частоти і фази вхідного сигналу відносно опорного коливання, низьку енергетичну ефективність, залежність від ефекту Допплера при застосуванні вказаної технології в мобільних мережах [3,4,5].

Системам OFDM властива довга посилка, яка дозволяє ефективніше послабити вплив багатопроменевості на завадостійкість прийому, і разом з тим, забезпечити високу сумарну швидкість передачі. Ці переваги зумовили одержати значний розвиток властивості

багатопроменевості на дротових каналах телекомунікаційних систем (ТС): довга посилка при порівняно високій стійкості відносно імпульсних завад і переривань. Крім того, параметри багатопроменевого сигналу, виходячи з припустимих відхилень амплітудно-частотних і фазо-частотних характеристик (АФЧХ) каналу ТС, вибираються такими, щоб система була нечутлива (інваріантна) до цих відхилень, чим би вони не були зумовлені. Тобто система будується на основі інваріантного підходу, що є позитивної властивістю систем передачі даних на основі технології OFDM [4,5]

Вирішення питання підвищення ефективності телекомунікаційних систем, що працюють на основі технології OFDM вимагаю обґрунтування подальших напрямків досліджень щодо удосконалення вказаної технології при умові збереження всіх притаманних їй властивостей, а саме інваріантності та високої завадостійкості.

Аналіз спектральної щільності одного елементарного OFDM-символу (Рис.1) та технології і теорії його побудови дозволяють визначити, що однією з груп параметрів, які можуть чинити вплив загалом на інваріантність системи та безпосередньо на її завадостійкість є положення та параметри кожної несучої. А саме, завадостійкость забезпечується кількістю під несучих, які повинні, в першу чергу займати своє положення в частотному розподілі OFDM-символу. В свої чергу, ці параметри необхідно розглядати як з точки зору розповсюдження радіолокаційної хвилі визначеної частоти і спектральної щільності сигналу, яка формує один канал передачі даних, так і з точки зору побудови дискретного сигналу, який передається цим каналом та має свої параметри [2,5].

Очевидно, зміна параметрів радіолокаційної хвилі каналу передачі даних може сформувати явище, яке визначається як між канальна завада. Сутність її полягає в впливу сусідніх несучих одна на одну через недодержання однією з несучих параметрів радіохвилі в заданих номінальних значеннях.

Дані обставини формують певний наукове завдання щодо обґрунтування методології зменшення впливу міжканальних завад в телекомунікаційних системах передачі даних на базі сигналу OFDM.

Питанню формування методології підвищення ефективності передачі даних на фоні забезпечення високої завадостійкості в телекомунікаційних системах, які працюють на основі використання сигналів OFDM присвячено ряд робіт.

Робота [6] присвячена розгляду математичної моделі побудови каналу зв'язку телекомунікаційної системи на базі сигналу OFDM при умові впливу навмисних завад. Запропонований в даній роботі механізм зменшення їх впливу направлений на удосконалення процесу мінімізації втрат частини даних з вхідного сигналу за рахунок введення часового захисного інтервалу та компенсування вказаної втрати даними з сусіднього каналу. Питання формування загальної методології зменшення такого роду негативних впливів та безпосередня втрата даних через міжканальні завади в даній роботі не висвітлені.

В роботі [7] розглянуто питання зменшення перешкоди в елементарному каналі передачі даних системи сигналу OFDM. Запропоновано, при умові врахування потужності внутрішньої канальної перешкоди, нове асиметричне вікно, яке забезпечує скорочення циклічного префіксу сигналу без зменшення потужності корисного сигналу. Певне питання обмеження впливу вказаних внутрішніх перешкод на сусідні канали в роботі розглянуто в частині, яка констатує можливості обраного методу щодо забезпечення обмеження впливу на потужність перешкоди в сусідньому каналі. Питання загального формування методології обмеження міжканальних завад в даній роботі не розглянуто.

Роботи [8,9] присвячені розгляду питання обмеження впливу поза смугових випромінювань в системах з ортогональним частотним поділом (OFDM). Певним чином такі випромінювання можна віднести до міжканальних завад але формуються вини випромінюваннями, які не несуть елементів корисних сигналів і, по суті являються зовнішніми перешкодами. Для їх зменшення в даних роботах запропоновано частотне спектральне попереднє кодування та нова структура прекодера, який забезпечує умови, що дозволяють приймачу вхідного сигналу використовувати класичний оцінювач каналу OFDM. Загальні підходи до зменшення такого роду перешкод та інших завад і збурень та методологія їх побудови в даних роботах не висвітлено.

Певні елементи методології зменшення міжканальних завад в OFDM сигналах висвітлено в роботі [10]. Розглянутий в роботі підхід до зменшення блокової діагоналізації перешкод

низхідної лінії зв'язку та розподілу потужності з урахуванням як відсутності, так і наявності інформації про стан каналу в багатокористувальницьких телекомунікаційних мережах на основі сигналів MIMO-OFDM певним чином стосується одного з проявів міжканальної завади але тільки в частині обмеження просторових перешкод. Безпосередній вплив відхилення параметрів одного з каналів та формування негативного впливу від нього на сусідні канали а також загальна методологія зменшення вказаного впливу в роботі не розглядалися.

Виконання досліджень

При побудові сигналу по технології OFDM необхідно вибирати чисельні значення таких параметрів, як число несучих гармонійних коливань (несучих), частотний інтервал між сусідніми несучими, захисний інтервал часу між сусідніми OFDM-символами, тривалість канального символу, спосіб модуляції коливання несучої, методи завадостійкого кодування. Значення перерахованих параметрів визначаються вимогами до самої системи, такими як смуга займаних частот, необхідна швидкість передачі інформації, значення розширення затримки й допплерівського розширення спектра сигналу в каналі. Деякі із цих вимог суперечливі [1,2,5]

Як було зазначено вище, OFDM-сигнал є сумою несучих гармонійних коливань (Рис.1), кожна з яких модулюється своїм підпотоком переданих біт з використанням фазової модуляції (ФМ) або квадратурної амплітудної модуляції (QAM). Нехай d_i – комплексне число, що представляє амплітуду $|d_i|$ й початкову фазу arg(d_i) *i*-го гармонійного коливання несучої OFDM-символу при використанні ФМ або QAM – символу. Кожний QAM-символ у системах цифрового радіозв'язку переносить кілька кодових біт. Якщо один OFDM – символ містить N_S носівних коливань, то можна вважати, що один OFDM-символ переносить блок *i* = 0, 1, 2,…, N_S-1 QAM-символів. Тоді комплексна обвідна одного OFDM-символу тривалістю *T* в момент часу t_k має вираз (1.1) [2,5]:

$$\dot{u}(t) = \sum_{i=0}^{N_S-1} d_1 exp\left\{ j2\pi \frac{i}{T}(t-t_k) \right\}, \quad t_k < t < t_k + T . \qquad (1)$$

Поза цим інтервалом часу OFDM-символ з номером *k* дорівнює нулю.

Вираз (1) описує граничний відеоеквівалент OFDM-радіосигналу.

Щоб одержати реальний OFDM – символ радіосигналу із прямокутною обвідною несучого гармонійного коливання частотою f_0, необхідно цілу й уявну частини обвідної виразу (1), що відповідає синфазної й квадратурної компонентам QAM – сигналу, помножити на cos(2πf_0t) і sin(2πf_0t) з наступним додаванням отриманих коливань [2,5].

З виразу (1) випливає, що для OFDM-сигналу інтервал між частотами сусідніх несучих $\Delta f = 1/T$, а частоти всіх несучих кратні цьому інтервалу. Отже, на тривалості одного OFDM-символу завжди укладається ціле число періодів кожної несучої. Для будь-яких сусідніх періодів число кожної несучої відрізняється на одиницю. Початкова фаза й амплітуда кожної несучої визначаються значенням трансльованого QAM-символу цієї несучої, а для різних несучих вони, звичайно, виявляються різними. У таких умовах когерентна демодуляція цього сигналу може бути здійснена з використанням взаємної ортогональності всіх несучих на інтервалі $t_k < t < t_k + T$ [2,5,11].

Наприклад, відповідно до класичної теорії потенційної завадостійкості для одержання оцінки QAM-символу d_i з номером l із прийнятої комплексної обвідної (1) (після її виділення в приймачі традиційним способом) необхідно помножити на коливання несучої $\exp\left\{ -j2\frac{l}{T}\pi(t-t_s) \right\}$ і результат проінтегрувати на інтервалі часу $t_k < t < t_k + T$ [5,11] :

$$\int_{t_k}^{t_k+1} \dot{u}(t)\exp\left\{-j2\pi\frac{l}{T}(t-t_k)\right\}dt =$$

$$= \int_{t_k}^{t_k+1} \exp\left\{-j2\pi\frac{l}{T}(t-t_k)\right\}\sum_{i=0}^{N_s-1} d_1\exp\left\{j2\pi\frac{i}{T}(t-t_k)\right\}dt = d_1T \quad .$$

Фактично відповідно до (2) при демодуляції одного OFDM – символу обчислюється значення спектральної щільності амплітуд даного символу на частоті $F_l = l\Delta f$ коливання несучої, з номером 1 [5,11].

На Рис.2 зображені спектри, які перекриваються різними несучими одного OFDM – символу і видно, що спектри всіх інших несучих на цій частоті дорівнюють нулю [2,5].

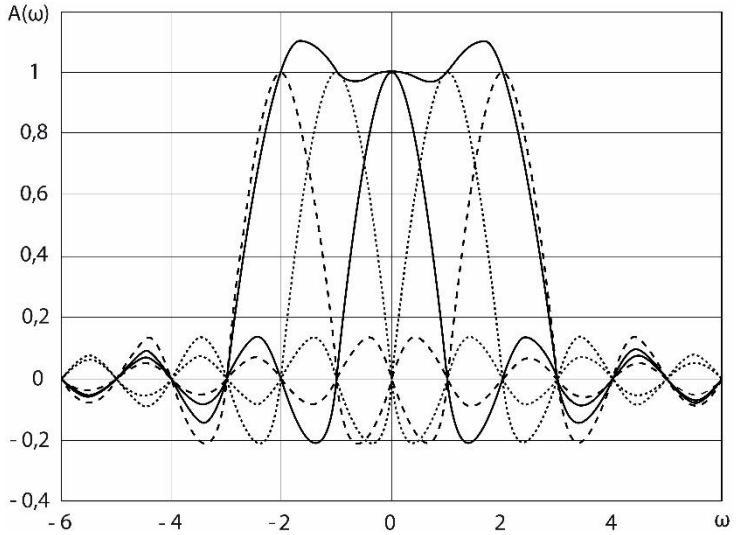


Рис. 2. Спектральна щільність суми п'яти несучих із однаковими амплітудами й початковими фазами

Таким чином, при визначеному виборі частот несучих коливань і інтервалу між сусідніми частотами, пов'язаного із тривалістю OFDM-символу (*T)*, забезпечується відсутність взаємних впливів між несучими [5,11,12].

Однією із основних властивостей технології OFDM є нечутливість до розширення затримки багатопроменевого сигналу. Ця властивість забезпечується за рахунок значного збільшення тривалості одного OFDM-символу, яка більша тривалості QAM-символу в значенні кількості піднесучих сигналу (N_S), тобто в N_S раз. При цьому відносний час збільшення затримки в каналі у стільки ж раз зменшується. Для того, щоб практично повністю усунути міжсимвольну інтерференцію між сусідніми OFDM – символами, вводиться захисний часовий інтервал T_g. Цей інтервал міг би зовсім не містити сигналу. Однак могла б виникнути міжканальна інтерференція між різними несучими, оскільки була б порушена їхня взаємна ортогональність. Причиною виникнення таких взаємних завад служить багатопроменевість [5,11].

Щоб усунути порушення ортогональності через багатопроменевість кожне несуче коливання циклічно триває на захисному інтервалі. У цьому випадку навіть затримка другого променя на деякий час *t* не приведе до порушення ортогональності між несучою першого променя та несучою іншого променя, оскільки на будь-якому інтервалі часу тривалістю *T* завжди буде укладатися ціле число періодів кожної несучої незалежно від розміщення цього інтервалу.

Це справедливо для будь-якого променя, якщо розширення затримки Δt через багатопроменевість каналу не перевищує тривалість захисного інтервалу T_g [11,12].

Після вибору захисного інтервалу можна знайти тривалість OFDM-символу T_c. Чим меншу частку інтервалу T_c становить тривалість захисного інтервалу T_g, тим менші енергетичні втрати, отже, менше необхідна випромінювана потужність для забезпечення необхідного значення відношення сигнал/завада в приймачі.

Однак тривалість T_c не може бути занадто великою, тому що кількість несучих стає значно більшою, а частотні інтервали між ними дуже малими. При цьому зростає чутливість системи до відхилень частоти в приймачі і до флуктуацій фази. Зростає також пікфактор OFDM-сигналу. Останнє ускладнює забезпечення лінійного режиму підсилювачів потужності сигналу в передавачах.

Тому вибір тривалості T_c символу може бути сформульовано в такий спосіб: якщо допустити енергетичні втрати не більші 1 дБ, то тривалість символу повинна бути більше захисного інтервалу принаймні в п'ять раз [5,11,12].

Отже, тривалість основного інтервалу інтегрування OFDM–символу в приймачі $T=T_c-T_g$, а, як було зазначено раніше, частотний інтервал між сусідніми несучими коливаннями $\Delta f = 1/T$.

Число несучих N_S можна визначити як $N_S = F/\Delta f$. З іншого боку, число несучих можна визначити як відношення сумарної швидкості передачі лінії R до швидкості передачі R_n на одній несучій.

У свою чергу, швидкість передачі на одній несучої визначається видом модуляції (наприклад, QAM-16), швидкістю використовуваного коду, швидкістю канальних символів. При знайденій швидкості проходження OFDM-символів і заданої швидкості передачі лінії можна обчислити число біт дискретного сигналу.

Число несучих є одним з найважливіших параметрів систем OFDM. Воно формує число підканалів (W) в структурі сигналу. Саме кількість підканалів W значною мірою формує та забезпечує інваріантність системи передачі даних OFDM.

За інших рівних умов з ростом W збільшується тривалість тактового інтервалу і знижується ефективно використовувана смуга частот, що в сукупності зменшує вплив неідеальності АФЧХ каналу. Однак, при цьому збільшується кількість операцій, що виконуються при модуляції і демодуляції сигналу, зростає вплив частотного розстроювання і фазового дрижання каналу [5,11,12].

Аналіз побудови сигналу за технологією OFDM, встановлення взаємозв'язку та взаємовпливу параметрів вказаного сигналу та сумісна взаємодія сусідніх каналів передачі даних в структурі одного сигналу дозволяють визначити наступний перелік важливих та критичних параметрів, які формують сам сигнал та, очевидно, можуть мати відношення до міжканальних завад.

До них відноситься:

– інтервал частот несучих коливань сигналу OFDM;

– частотна невизначеність вхідного сигналу (формує відхилення АФЧХ та мінімізується побудовою каналу прийому вхідного сигналу);

– кількість несучих в одному сигналі OFDM;

– початкова фаза та амплітуда кожної несучої;

– частотний інтервал між сусідніми несучими;

– часовий інтервал когерентної демодуляції сигналу OFDM при умові взаємної ортогональності всіх несучих сигналу;

– часовий інтервал тривалості OFDM-символу;

– захисний часовий інтервал, що забезпечує міжсимвольну інтерференцію при прийомі багатопроменевих сигналів та є складовим часового інтервалу OFDM-символу.

Як було зазначено раніше, збільшення кількості піднесучих збільшує кількість операцій, що виконуються при модуляції і демодуляції сигналу. А при цьому зростає вплив частотного розстроювання і фазового дрижання каналу [11,12,13]. Через ці ефекти несуча зміщується з встановленого частотного положення, тобто формується міжканальна завада, вплив якої, як радіотехнічного збурення, можна оцінити по її потужності.

Виходячи з цього, в якості методологічного підходу до зменшення рівня міжканальних завад в телекомунікаційних системах передачі даних на базі сигналу OFDM можна сформувати по наступному алгоритму.

1. Основний критерій оцінки зменшення впливу – потужність міжканальної завади;

2. При визначенні потужності міжканальної завади прийняти фіксованими наступні параметри:

– смугу пропуску каналу;

– швидкість передачі повідомлення;

– кратність модуляції.

– АЧХ і ФЧХ каналу прийняти в вигляді нормованих шаблонів для кожного числа переприйомів вхідного сигналу OFDM.

3. Вибір захисного інтервалу прийому вхідного сигналу демодулятором для обмеження перехідних процесів, що виникають на кордоні тактових інтервалів;

4. Створення моделі прийому вхідного сигналу як суми корисного сигналу та компонентів міжканальних завад. Вказана модель повинна однозначно пов’язувала відстань між піднесучими, їх кількість та значення захисного інтервалу при умові мінімізації потужності міжканальної завади.

Висновки

1. Проведено аналіз структури сигналу OFDM та визначено, що одним з факторів, який може вплинути на ефективність передачі даних за допомогою вказаної технології є положення та параметри кожної піднесучої з складу даного OFDM-символу.

2. Визначено, що зміна положення та параметрів піднесучої з складу даного OFDM-символу створюють вплив однієї піднесучої на іншу. Таке явище визначається як міжканальна завада, яка характеризується величиною потужності.

3. Встановлено, що кількість під несучих в структурі сигналу забезпечує інваріантність системи до зовнішніх збурень та перешкод, але створює умови формування міжканальних завад, ріст яких пов'язаний з збільшенням кількості піднесучих в структурі даного OFDM-символу.

4. Запропоновано методологічний підхід до зменшення рівня міжканальних завад телекомунікаційних системах передачі даних на базі сигналу OFDM, визначено критерій оцінки ефективності та алгоритм реалізації поданого методологічного підходу.

Література

1. Попівський В.В., ,Лемешко О.В., Ковальчук В.К. Плотніков М.Д., Картушин Ю. П. та інші Телекомунікаційні системи та мережі. Структура й основні функції. Том 1..URL: http://www.znanius.com/3534.html.

2. Балашов В. О., Воробієнко П. П., Ляховецький Л. М., Педяш В. В. Системи передавання широкосмуговими сигналами. Одеса: Вид. центр ОНАЗ ім. О.С. Попова, 2012. 336 с.

3. Бакулин, М. Г.,. Крейнделин В.Б., Шлома А.М.,. Шумов А.П. Технология OFDM. М.: Горячая линия - Телеком, 2015. 60 с.

4. Мазурков, М.И. Системы широкополосной радиосвязи. Одесса: Наука и техника, 2010.340 с.

5. Скляр Б. Цифровая связь. Теоретические основы и практическое применение.. Москва: Издательский дом «Вильямс», 2003. 1099 с.

6. Зайцев С.В. Математичні машини і системи.Київ: 2011.№ 4. С. 166–175.

7. Taheri, T. Nilsson, Van de Bee J .Asymmetric Transmit-Windowing for Low-Latency and Robust OFDM /T. Taheri, R. k // 2016 IEEE Globecom Workshops (GC Wkshps). –Washington, DC USA, 2016. pp. 1-6.

8. Mohamad, M, Nilsson. R., De Beek A Novel J. Van. Transmitter Architecture for Spectrally-Precoded OFDM / M. Mohamad, IEEE Transactions on Circuits and Systems I: Regular Papers. –Beijing, China, Aug. 2018. –Vol.65, №8.pp. 2592-2605.

9. Beek, J. OFDM Spectral Precoding with Protected Subcarriers .IEEE Communications Letters. Paris: December 2013. –Vol.17, №12, pp. 2209-2212.

10. Agrahari, A. ,. Agrahari A,. Varshney P. Jagannatham Precoding and Downlink Beamforming in Multiuser MIMO-OFDM Cognitive Radio Systems With Spatial Interference Constraints . IEEE Transactions on Vehicular Technology. Sydney: March 2018. Vol.67, №3.pp. 2289-2300.

11. Гусєв, О.Ю. Конахович Г.Ф,. Корнієнко В.І, Кузнецов Г.В.,. Пузиренко О.Ю. Теорія електричного зв’язку..Львів: Магнолія , 2010. 364 с.

12. Стеклов, В.К., Беркман Л.Н. К.: Техніка, 2006. 552 с.

13. Beek, J.J. Sandell M., Borjesson P.O. ML Estimation of Timing and Frequency On-set in Multicarrier Systems . Lulea, Sweden : University of Technology, 1996. 32 p.

References

1. Popivs'kyy V.V., P. P. Vorobiyenko, L. M. Lyakhovets'kyy, V. V. Pedyash Lemeshko O.V., Koval'chuk V.K.,. Plotnikov M.D.,. Kartushyn Y.P. ta inshi Telekomunikatsiyni systemy ta merezhi. Struktura ta osnovni funktsiyi .[Telecommunication systems and networks. Structure and main functions] Tom 1 http://www.znanius.com/3534.html.

2. Balashov, V. O. Systemy peredavannya shyrokosmuhovymy syhnalamy. [Broadband signal transmission systems] Odesa: Vyd. tsentr ONAZ im. O.S. Popova, 2012. −336 s.

3. Bakulin, M. H.,. Kreyndelin V.B., Shloma A.M.,. Shumiv A.P. Tekhnolohiya OFDM.[OFDM technology] .M.: Haryacha liniya - Telekom, 2015. - 60 s.

4. Mazurkov, M.I. Systemy shyrokosmuhovoho radiozv'yazku.[Broadband radio communication systems]. Odesa: Nauka ta tekhnika, 2010. -340 s.
5. Sklyar, B. Tsyfrovyy zv'yazok. Teoretychni osnovy ta praktychne zastosuvannya. [Theoretical foundations and practical application] -Moskva: Vydavnychyy budynok «Vil'yams», 2003.-1099 s.
6. Zaytsev, S.V. Matematychna model' kanalu zv'yazku iz syhnalamy OFDM ta navmysnymy zavadamy Matematychni mashyny ta systemy. [Mathematical model of a communication channel with OFDM signals and intentional interference].Kyyiv: 2011.№ 4. S. 166-175.
7. 7. Taheri, T. Nilsson, Van de Bee J Asymmetric Transmit-Windowing dlya Low-Latency and Robust OFDM /T. Taheri, R. Nilsson, J. van de Beek // 2016 IEEE Globecom Workshops (GC Wkshps). -Washington, DC USA, 2016. -P. 1-6.
8. Mohamad, M, Nilsson. R., De Beek A Novel J. Van. Transmitter Architecture dlya Spectrally-Precoded OFDM / M. Mohamad, R. Nilsson, J. Van De Beek // IEEE Transactions on Circuits and Systems I: Regular Papers. -Beijing, China, Aug. 2018. -Vol.65, №8. -P. 2592-2605.
9. Beek, J. OFDM Spectral Precoding with Protected Subcarriers / J. Van De Beek // IEEE Communications Letters. - Paris, December 2013. -Vol.17, № 12, -P. 2209-2212.
10 Agrahari, A. ,. Agrahari A,. Varshney P. P. Precoding and Downlink Beamforming v Multiuser MIMO-OFDM Cognitive Radio Systems z Spatial Interference Constraints / A. Agrahari, P. Varshney, A. K. Jagannatham // IEEE Transactions on Vehicular Technology. -Sydney, March 2018. -Vol.67, №3. -P. 2289-2300.
11. Husyev O.Yu. ,.Konakhovych H.F. Korniyenko, V.I,. Kuznyetsov H.V. Teoriya elektrychnoho zv'yazku . [Theory of electrical communication].L'viv: Mahnoliya 2006, 2010. 364 s.
12. Steklov, V.K., Berkman L.M. Teoriya elektrychnoho zv'yazku: Pidruchnyk dlya VNZ .[Theory of electrical communication: Textbook for universities] K.: Tekhnika, 2006. - 552 s.
13. Beek, JJ. ML Estimation of Timing and Frequency On-set v Multicarrier Systems / J.J. Beek, M. Sandell, P.O. Borjesson. - Lulea, Sweden: University of Technology, 1996. - 32 p.

УДК 621. 391. 814

ОПТИМІЗАЦІЯ ПРОЕКТУВАННЯ ЕФЕКТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ІЗ ВРАХУВАННЯМ ПРОПУСКНОЇ ЗДАТНОСТІ ТА БІТОВИХ ПОМИЛОК

DOI 10 36994 / 2788- 5518- 2022-02-04-11

Пелішок В.О., *д.т.н.,проф. Національний університет «Львівська політехніка» Львів, Україна. volodymyr.o.pelishok@lpnu.ua.*

Чайковський І.Б., *к.т.н., доц. Національний університет «Львівська політехніка» Львів, Україна. Ihor.b.chaikovskyi@lpnu.ua.*

Масюк, А.Р.,*к.т.н., доц. Національний університет «Львівська політехніка» Львів, Україна. andrii.r.masiuk@lpnu.ua.*

Андрухів Т.В, *к.т.н. Лльвівська філія ПАТ «Укртелеком», Львів, Україна. tandrukhiv@ukrtelecom.ua*

Анотація: *головною вимогою до телекомунікаційних систем передавання цифрової інформації різного призначення є забезпечення її якісних характеристик: швидкості передавання, пропускної здатності, ймовірності бітової помилки. Ці характеристики знаходяться у складній взаємній залежності, що вимагає необхідність досліджень із використанням спеціальних підходів і методів. В роботі розглянуто та запропоновано шляхи оптимізації процесу проектування та вибору серед можливих варіантів реалізації більш ефективних систем.*

Ключові слова*: телекомунікаційна система, пропускна здатність, бітова помилка, суміщені графіки.*

DESIGNING OPTIMIZATION OF EFFICIENT TELECOMMUNICATION SYSTEMS WITH CONSIDERATION BANDWIDTH AND BIT ERRORS

Volodymyr Pelishok*, Dr.habil, Prof. Lviv Polytechnic National University, Lviv, Ukraine. volodymyr.o.pelishok@lpnu.ua.*

Ihor Tchaikovskyi*, PhD, Ass. Prof. Lviv Polytechnic National University, Lviv, Ukrain. Ihor.b.chaikovskyi@lpnu.ua.*

Andriy Masiuk*, PhD, Ass. Prof. Lviv Polytechnic National University, Lviv, Ukraine. andrii.r.masiuk@lpnu.ua.*

Taras Andrukhiv*, Ph.D.Lviv branch of the PJSC "Ukrtelecom", Lviv, Ukrain., tandrukhiv@ukrtelecom.ua.*

Abstract*: main requirement to telecommunications for the transmission information of various purposes is to ensure its quality characteristics: speed, bandwidth and probability of bit error. These characteristics are in a complex mutual dependence, which requires the need for research using special approaches and methods.*

A feature of the designing aspects of modern telecommunications is providing BER level and bandwidth. Thus, it is necessary to provide the system with certain resources: the bandwidth of the channel, the number of signal levels and SNR. Each of the specified parameters is characterized by significant features.

The paper considers two important components related to the implementation of telecommunications - design optimization and selection of more effective systems implementation options among possible one.

Design optimization is carried out using modern software packages, which brings the design closer to the automated one. An analytical-graphical approach is also widely used, in which complex analytical transformations are replaced by eq uivalent graphic transformations. At the same time, the design process is practically not complicated and provides the possibility of visual perception of the essence of signal processing in individual nodes. The following ways of optimization are proposed: determination of the probability of erroneous receiving of bits information signals using specialized means; the use of the "2D-3D-2D/" method, which allows to simplify the formation of the necessary graphic dependencies; application-combined graphics that allow you to replace the need for the inconvenient use of two graphic windows with the convenience of using one graphic window.

On the basis of the conducted research, an algorithm for the design of effective telecommunications was developed, which allows in each specific case to obtain all possible variants of effective (according to the proposed criterion) one; form a criterion for choosing a more effective one among the received options.

***Key words**: telecommunications, optimization, bandwidth, BER, combined graphs.*

Вступ

Одним із важливих аспектів проектування цифрових телекомунікаційних систем (ТКС) є забезпечення (рис.1) двох основних (вихідних) параметрів:

- ймовірності появи бітових помилок Pb (або BER, Bit Error Rate), тобто помилкового прийняття «1» замість переданого «0» і навпаки;
- пропускної здатності C (біт/с), яка вказує максимальну швидкість (Rmax) передавання даних.

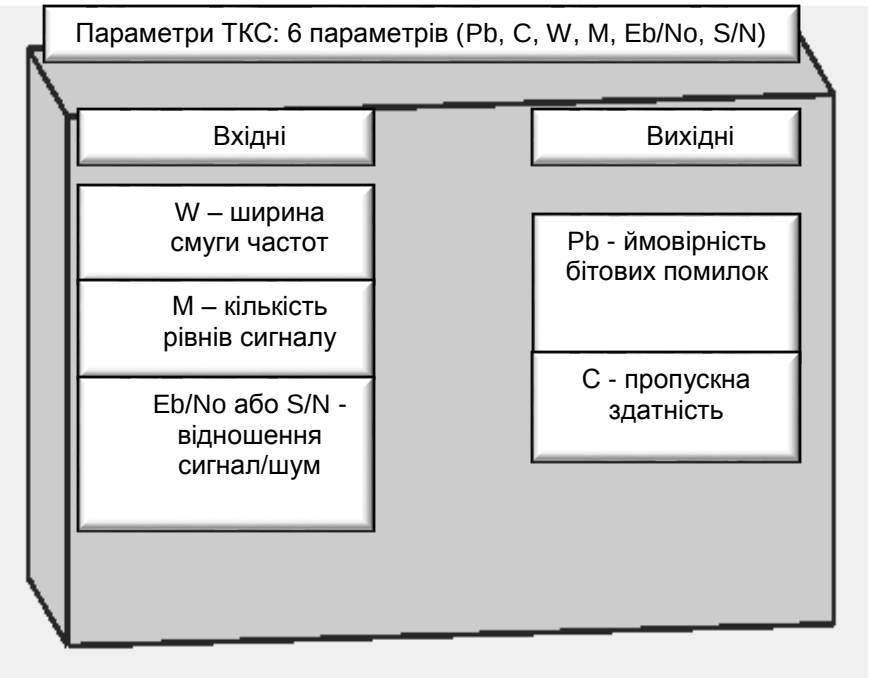


Рис.1. Основні параметри ТКС

Для їх реалізації системі необхідно надати певні ресурси (вхідні параметри):

- ширину W (Гц) смуги частот каналу зв’язку;
- кількість M рівнів сигналу;
- відношення сигнал/шум, яке прийнято використовувати в одному з двох видів - S/N (відношення потужності сигналу до середньої потужності шуму), або Eb/No (відношення енергії біта до спектральної густини потужності шуму).

Кожен із 6-и вказаних параметрів характеризується суттєвими особливостями [1, 2], причому більш простими є вхідні параметри.

Ширина смуги частот каналу зв'язку. Вказаної смуги завжди недостатньо. На її основі формується один із основних показників, що характеризують ефективність ТКС.

Кількість рівнів сигналу. Кожен біт вхідної інформації можна передавати окремо (наприклад 1, 0, 0, 1 і т. д.), або з k бітів формувати символи і далі передавати тільки символи. Наприклад, якщо символ містить k=2 біти, то можливі M=4 варіанти розміщення бітів у символі (00, 01, 10, 11). При передаванні різним символам необхідно присвоїти специфічну ознаку (різний рівень сигналу). Інакше на приймальній стороні буде неможливо отримати інформацію про вміст бітів в отриманому символі. На рис.2 приведено приклад формування 4-х рівневого (M=4) сигналу різними рівнями.

Рис.2. Формування M-рівневого сигналу при k=2

У загальному випадку очевидною [2] є залежність

$$M=2^k \qquad (1,а)$$

або $$k=\log_2(M) \qquad (1,б)$$

На рис. 3 приведено фрагмент графічного відображення залежності (1,а)

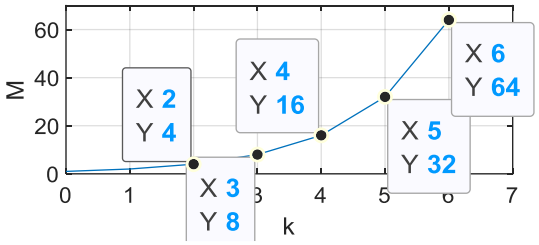


Рис.3. Залежність M(k) для M-рівневого сигналу

Видно, що значення k, M можуть приймати тільки дискретні значення. Вказана особливість формує певні специфічні обмеження, які необхідно враховувати при проектуванні ТКС.

У випадку заданого значення одного з параметрів (W=const або C=const) другий також може отримувати (1,а) тільки дискретні значення. При проектуванні ТКС часто можна отримати розраховані значення, які не співпадають з вказаними дискретними. Рекомендації для таких випадків практично відсутні у відомих дослідженнях.

Відношення сигнал/шум може бути представлене одним із двох варіантів (S/N, або Eb/No), між якими є [1] відомий взаємозв’язок :

$$Eb/No= (S/N)/(C/W) \qquad (2,а)$$

або $$S/N = (Eb/No)(C/W) \ . \qquad (2,б)$$

Не є очевидним, якому з варіантів слід надати перевагу при проектуванні ТКС. У відомих наукових джерелах такі рекомендації також відсутні.

Ймовірність бітових помилок Pb для бінарних систем визначається на основі інтеграла Гауса Q(x):

$$Pb = Q(x) , \quad (3)$$

де: $Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{u^2}{2})\, du$; x=(a*Eb/No)$^{1/2}$; a=2 для біполярного сигналу; a=1- для уніполярного сигналу.

Таким чином, значення P_b залежить (3) від виду використаних сигналів (уніполярного чи біполярного) приведених на рис.4

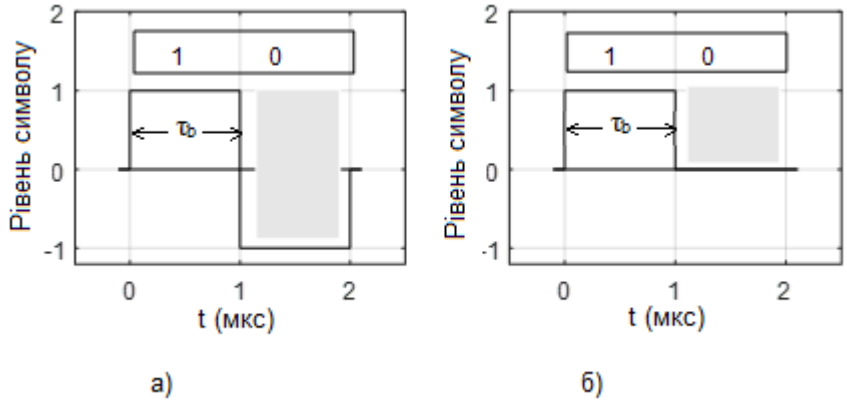


Рис. 4. Вид сигналу: а) біполярний; б) уніполярний

Застосування різних видів сигналу (уніполярний або біполярний) спричинене тим, що цифрові дані в початковому виді (наприклад, письмові 01101 і т.д.) не придатні для передавання мережами ТКС. Їх необхідно попередньо перетворити в біти електричного сигналу. Найбільш поширені варіанти електричного сигналу: біполярний сигнал NRZ-L (без повернення до нуля) та уніполярний RZ - (із поверненням до нуля). На рис. 4, як приклад, приведено відображення бітів, що відповідають 1 і 0, причому тривалість біта τ_b=1мкс.

Варто зауважити, що залежність Pb(Eb/No) отримана на основі інтеграла помилок (3), залежить від виду використаного сигналу

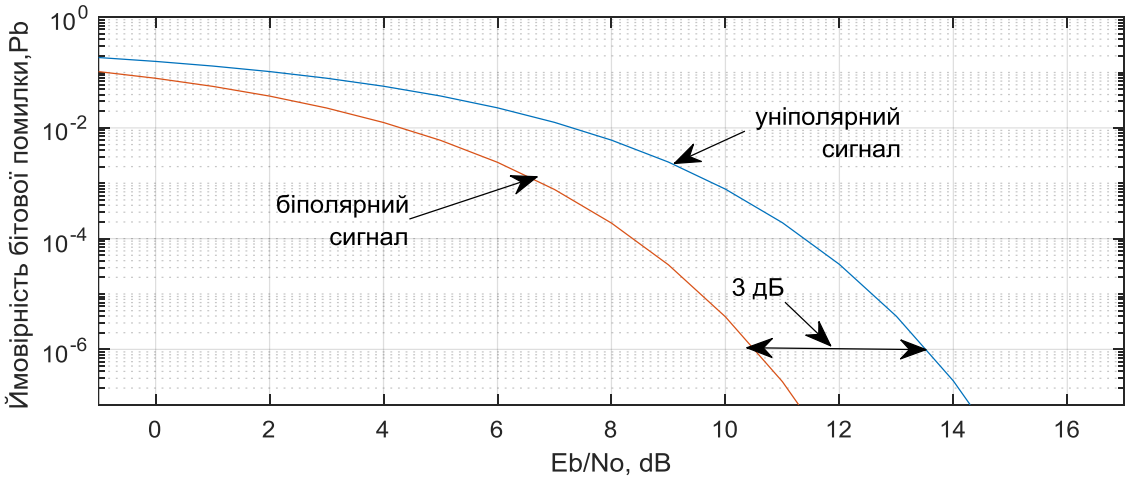


Рис.5. Залежність Pb(Eb/No) для уніполярних та біполярних сигналі

Видно, що для забезпечення Pb≈10^{-6} при використанні біполярного сигналу достатньо відношення Eb/No на 3 дБ меншого (позитивний ефект) порівняно з уніполярним сигналом. Тому далі використовуються тільки біполярні сигнали, як більш ефективні.

Часто до проектованих ТКС задається вимога (Pb ≤ Po, де Po – максимально допустиме значення Pb). Тоді:

$$Pb = Po \quad . \tag{4}$$

Слід зазначити, що визначення Pb досить трудомістке. Для цього в [1] навіть пропонується використовувати спеціальні громіздкі таблиці, що потребує значної затрати часу необхідного для побудови (рис.5). На основі вказаного прикладу видно, наскільки актуальною є подальша оптимізація процесу проектування ТКС.

Ймовірність бітових помилок Pb для М-рівневих систем. На практиці, крім бінарних систем, також широко використовуються М-рівневі системи. В них застосовуються символи, для яких справедливі залежності (1,а,б). Тому при аналізі М-рівневих систем спочатку визначається ймовірність символьних помилок Ps . Далі на їх основі можна також визначити ймовірність бітових помилок Pb.

Для ортогональних сигналів з когерентним детектуванням ймовірність символьних помилок становить [1]:

$$Ps(M) \le (M-1)Q(Es/No)^{1/2} \quad , \tag{5}$$

де $Es = Eb(\log_2 M) = Eb*k$ – енергія одного символу.

На рис.6 показана залежність (6) для різних видів М-рівневих систем.

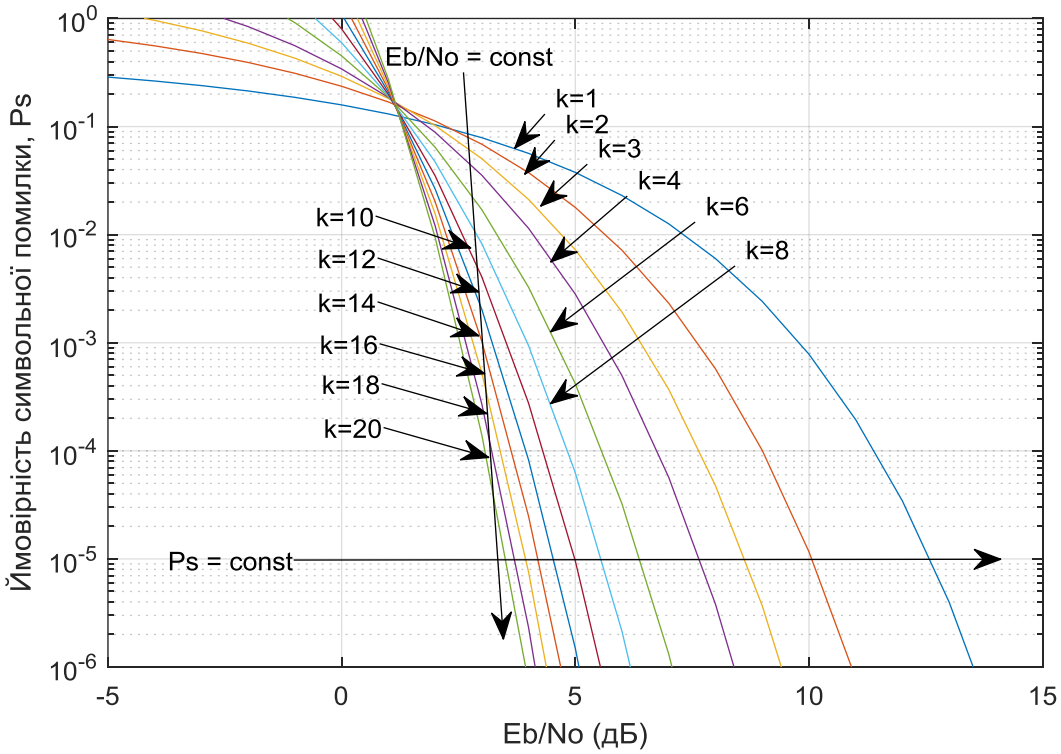


Рис.6. Ймовірність символьної помилки для М-рівневого ортогонального передавання сигналів із когерентним детектуванням.

Видно, що при збільшенні k, наявні позитивні ефекти:

- зменшується рівень сигналу (Eb/No), необхідний для забезпечення необхідного значення Ps=const;
- або зменшується значення Ps при заданому значенні Eb/No =const.

На основі отриманих значень Ps(M) можна визначити ймовірність бітових помилок Pb:

$$Pb/Ps = 2^{k-1}/(2^k - 1) = (M/2)/(M-1) \quad . \qquad (6)$$

Варто зауважити, що при значному збільшені k залежність (6) навіть спрощується:

$$Pb/Ps \approx 0.5 \quad . \qquad (7)$$

Інформація (рис.6) корисна для оцінки впливу різних рівнів М – арних сигналів на якість переданих даних. При проектуванні зацікавлення часто полягає в більш конкретній залежності (наприклад, Eb/No (M)) при Ps = const. Отримати вказану залежність, використовуючи рис.6, можна але досить складно та незручно.

Однією зі залежностей для пропускної здатності С є формула Найквіста. Вона вказує, що значення С можна суттєво збільшити (що завжди є бажаним) навіть при W=const у випадку використання М-рівневих сигналів:

$$C=2W*\log_2(M) \quad , \qquad (8)$$

Один із показників ефективності ТКС (Cn) формує пропускна здатність С та смуга частот W:

$$Cn=C/W \quad . \qquad (9)$$

Як видно, Cn вказує на швидкість передачі даних, яку забезпечує система при використанні одиниці смуги частот. Тобто, вказаний параметр оцінює як ефективно ТКС використовує дефіцитний ресурс смуги частот. Значення Cn залежить, згідно залежностей (10) та (1,б), від кількості k бітів, яка міститься в символі (табл.1)

Таблиця 1

k	1	2	3	4	5	6	7
Cn	2	4	6	8	10	12	14

Можна зауважити, що забезпечення максимального значення Cn, є одним із визначальних факторів вибору ефективних ТКС, що вирішується в даній роботі.

Як видно (рис.6 та залежність (9)) використання М-рівневих сигналів із більшим значенням М забезпечує лише позитивні результати. Проте певні обмеження для такого збільшення М накладає відношення сигнал/шум.

Другою залежністю для пропускної здатності С є формула Шеннона. Вона вказує вплив на пропускну здатність С смуги частот каналу W та відношення сигнал/шум:

$$C = W * \log_2(1 + \frac{S}{N}) \quad . \qquad (10)$$

Отже, збільшити пропускну здатність можна шляхом збільшення як смуги частот W, так і збільшенням відношення сигнал/шум.

При використанні формули Шеннона у відомих дослідженнях подаються певні необґрунтовані дані та навіть неточності. Зокрема в [1], з 4-х можливих графічних зображень залежності (10) приведено три:(Cn(S/N), 1/Cn(S/N) та 1/Cn(Eb/No). Як показано далі саме пропущений варіант, тобто Cn(Eb/No) найбільш доцільно використовувати при оптимальному проектуванні. Крім того, в [1] у математичних перетвореннях залежності (11), з метою визначення границі Шенона, допущено неточності

Багатоваріантність підходів до оптимального проектування ефективних ТКС. Дані про вище описані загальні відомості відносно ТКС систематизовані (рис.7). При цьому враховано, що відношення сигнал/шум можна характеризувати двома варіантами і не є очевидним якому варіанту доцільно надати перевагу.

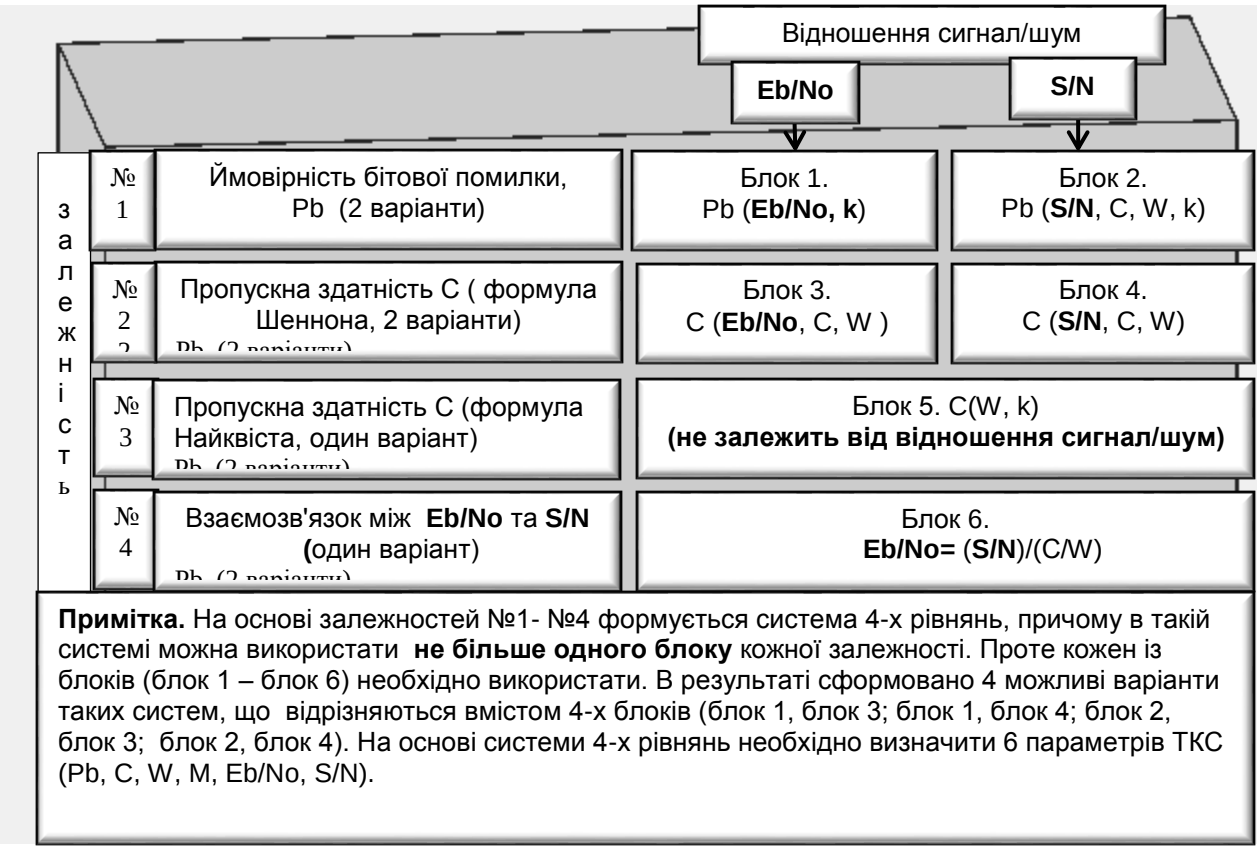


Рис.7. Основні залежності, необхідні для проектування ТКС

Використовуючи систему 4-х рівнянь можна визначити значення лише 4-х невідомих параметрів. Тому значення решти 2-х (6-4) параметрів необхідно попередньо задати. Кількість V_1 варіантів вибору заданих параметрів у даному випадку досить значна (визначається числом сполучень із 6-и параметрів по 2-а) та становить [10] $V_1=B_6^2$ =15 варіантів. На рис.6 вказано, що кількість можливих варіантів системи 4-х рівнянь також становить 4. Отже, кількість необхідних варіантів систем рівнянь для розгляду (з метою розробки алгоритму оптимізації проектування та відбору ефективних ТКС) повинна становити 4*15=60 варіантів.

Таким чином, постає потреба щодо зменшення кількості варіантів ТКС (серед можливої їх кількості, тобто 60 варіантів), достатніх для вибору більш ефективної ТКС.

В результаті проведеного аналізу показано, що при дослідженнях окремих складових ТКС мають місце суттєві недоліки. Їх частково або повністю усуває запропонована методика.

Особливості запропонованої методики. Як видно з вище приведених висновків, двом аспектам реалізації ТКС приділялось недостатньо уваги, а саме:

- оптимізації проектування окремих складових ТКС (частина 1);
- вибору більш ефективних ТКС при фактичній відсутності алгоритму їх оптимального проектування (частина 2).

Вказані проблеми частково або повністю вирішені та вдосконалені запропонованою методикою. Її основні особливості приведені в табл.2

Оптимізація проектування окремих складових ТКС

Визначення ймовірності помилок Pb

Як вказувалось вище, визначення ймовірності помилок (3) досить складне. Тому для суттєвого спрощення отримання Pb пропонується використовувати можливості програмних пакетів, наприклад MATLAB [5, 6], залежності (рис.3, рис.5, рис.6 і т.д.).

Таблиця 2

Частина 1. Оптимізація проектування окремих складових ТКС			**Частина 2.** Оптимізація проектування ТКС в цілому. Вибір більш ефективних варіантів ТКС. Розробка алгоритму проектування.
Засіб 1. Стосовно ймовірності помилок, Pb	**Засіб 2.** При аналізі сімейства залежностей (наприклад, рис.6)	**Засіб 3.** При сумісному використанні двох різних функцій спільного аргументу	

Додатковою перевагою використання таких графічних залежностей є можливість у процесі проектування визначати їх значення в довільній точці (наприклад, рис.3). Така можливість наближує процес проектування до автоматизованого. В перспективі, при такому проектуванні, змінювати параметри ТКС буде можливо використовуючи програмні засоби зв'язку.

Аналіз сімейства залежностей

Таким є , наприклад, сімейство (рис.6), отримане на основі формули (5). Вона містить інформацію про взаємозв'язок між 3-а, в принципі рівноцінними параметрами (Pb, (Eb/No), k). Використавши один параметр (Eb/No) - як аргумент, другий параметр (Pb) – як функцію, отримано сімейство залежностей рис.6 – при різних значеннях k (k1, k2, k3 і т.д.).

Але, як показано далі, при проектуванні ТКС представляють інтерес також інші сімейства залежностей, отримані на основі формули (5), зокрема рис.8

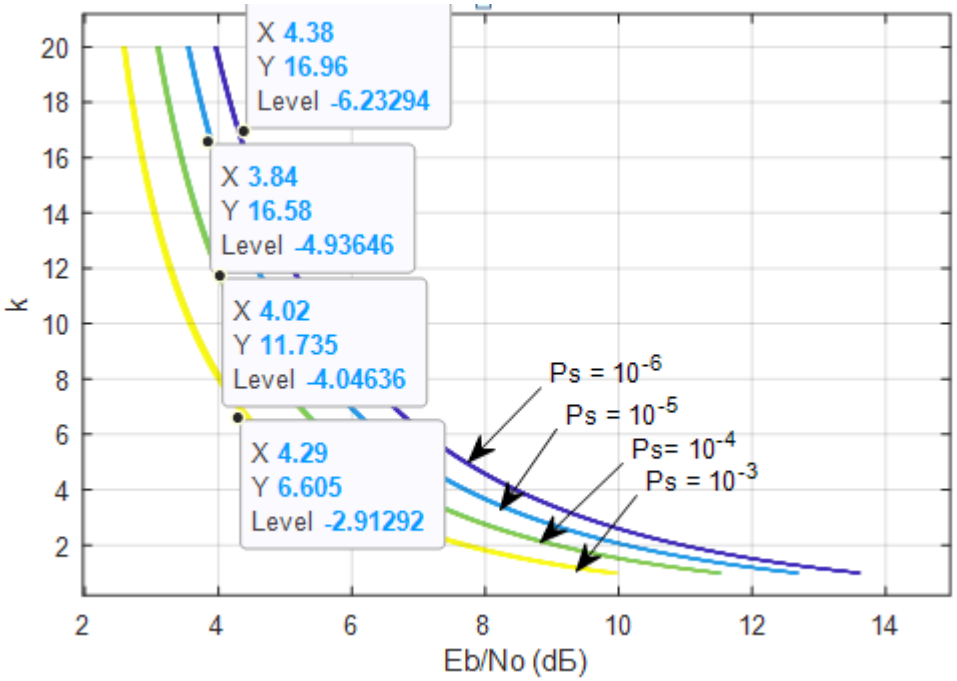


Рис.8. Залежності k(Eb/No) при Ps=const

Здавалось би, залежності (рис.8) можна отримати аналогічно, як і залежності (рис.6). Але це неможливо, тому що для такої побудови значення функції (Pb –для рис.6, k – для рис.8) повинно бути отримано (формула 5) в «явному» виді (в лівій частині рівняння) . Якщо для Pb це виконується, то для k отримати його в «явному» виді неможливо.

Вирішити вказану проблему можна використовуючи метод « 2D – 3D – 2D/ », запропонований в [4]. Його цінність в тому, що він дозволяє складні (часом і неможливі) аналітичні перетворення

замінити еквівалентними їм (але простими) графічними перетвореннями. Вказаний метод містить 3 етапи. На 1-му етапі (2D) формується необхідне сімейство залежностей на площині (для даного прикладу – це сімейство рис.6). На другому етапі основний недолік усувається (рис.6) наступним чином - кожна з сусідніх залежностей (при k = const) штучно «розсувається» одна від одної шляхом формування (3D) просторової залежності

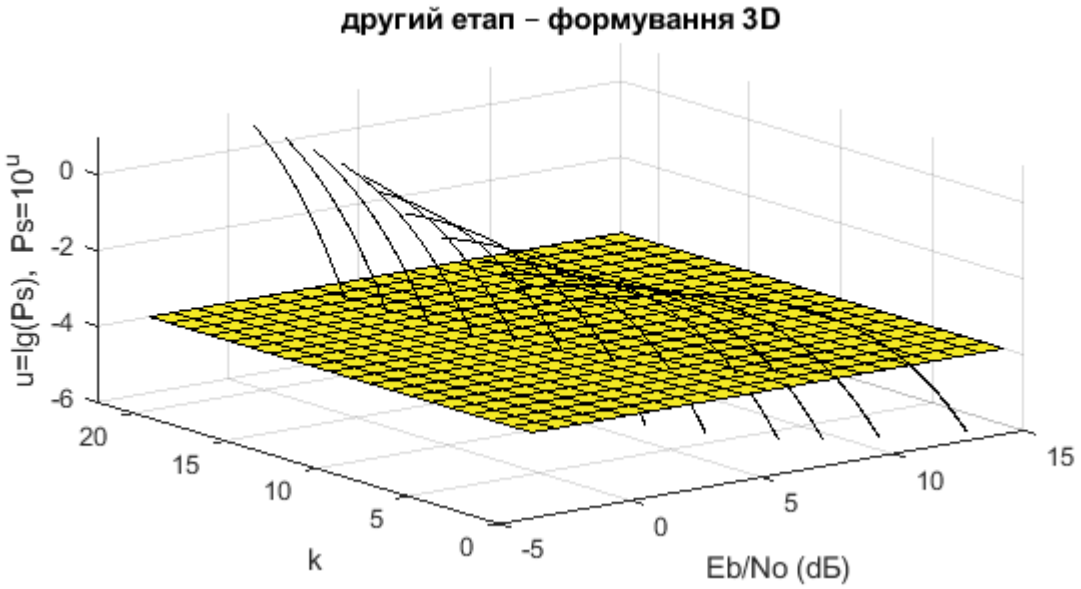


Рис.9. Другий етап методу « 2D - 3D – 2D/ »

Незважаючи на більшу складність рис.9 порівняно з рис.6 обсяг обчислень при цьому практично не збільшився. Це однакові обчислення для кожної залежності (при k = const) тільки різно розміщені.

На рис.9 також приведена додаткова горизонтальна площина, наприклад, при $Ps=10^{-4}$. Лінія її перетину з сімейством залежностей при k = const якраз і формує одну зі залежностей (при $Ps=10^{-4}$ на рис.8). Формуючи послідовно горизонтальну площину на інших рівнях ($Ps=10^{-6}$, $Ps=10^{-5}$, $Ps=10^{-3}$) отримано аналогічно інші залежності (рис. 8).

На третьому етапі на основі даних (рис.9) формується ($2D^{/}$) шукана залежність на площині (рис.8). Для цього достатньо здійснити проєкцію даних (рис.9) на горизонтальну площину. Взагалі можливості методу « 2D – 3D – $2D^{/}$ » багато ширші та виходять за межі даної роботи.

Сумісне використання (в одному графічному вікні) двох різних функцій спільного аргументу. В даному випадку пропонується використання суміщених графіків, що суттєво спрощує процес проектування. Їх побудова та використання показано далі про розгляді прикладів проектування конкретних ТКС.

Оптимізація проектування ТКС у цілому

Зменшення кількості варіантів систем рівнянь необхідних для вибору ефективних ТКС. При аналізі даних (рис.7) показано, що їх кількість досить значна (60 варіантів). Тому постає питання їх суттєвого зменшення. Вказане зменшення кількості варіантів ТКС здійснюється поетапно.

На першому етапі здійснюється поділ 6-и параметрів, які потрібно визначити (рис.7), на дві групи: які потрібно визначати в 1-у чергу (2-у чергу). Для цього формула Найквіста (8), яку містить також блок 5 (рис.7) модифікується (з врахуванням залежностей (1,а), (1,б) та (9)) наступним чином:

$$Cn = C/W = 2k \quad . \qquad (11)$$

Далі в блоках (2-6 (рис.7)), які містять параметри C та W, здійснюється заміна даних параметрів згідно (11) на параметр k. В результаті з 6-и параметрів (рис.7) залишається 4-и (Pb,

k, (Eb/No), (S/N)), які необхідно визначати в першу чергу. Завдяки тому, що вказані 4-и параметри отримані з використанням формули Найквіста (тобто блоку 5 залежності №3 (рис.7), відпадає потреба у використанні блоку 5 при формуванні системи рівнянь.

Таким чином, у результаті виконання даного етапу, отримано наступні спрощення:

- кількість параметрів, які необхідно визначати в першу чергу, зменшилась з 6-и до 4-х;
- кількість рівнянь в системі, необхідна в даному випадку, зменшилась із 4-х до 3-х.

На другому етапі відбувається подальше зменшення кількості параметрів, які необхідно визначати першочергово, та кількість рівнянь необхідних для цього. Аналіз показує, що з 4-х можливих варіантів систем рівнянь (рис.7) доцільно використовувати тільки два варіанти, які містять інформацію: про відношення сигнал/шум в однаковому виді ((Eb/No) або (S/N)), тобто:

- варіант 1 (блок 1 та блок 3, які мають тільки відношення (Eb/No) та не містять відношення (S/N);
- варіант 2 (блок 2 та блок 4, які містять тільки відношення (S/N) та не містять відношення (Eb/No).

Варто зазначити, що варіанти (1 та 2) інформаційно рівноцінні, причому трудомісткість їх використання практично однакова. Тому далі достатньо використовувати тільки один із них. Унаслідок із тим, що більш поширеним [1] є використання відношення сигнал/шум у виді (Eb/No), доцільно використовувати варіант 1. Враховуючи те, що варіант 1 не містить параметра (S/N), немає потреби використовувати залежність №4 блок 6 (рис.7) у системі рівнянь.

Отже, в результаті другого етапу, отримано спрощення:

- кількість параметрів, які необхідно визначати в першу чергу, зменшилась з 4-и до 3-х (Pb, k, (Eb/No));
- необхідна кількість рівнянь в системі зменшилась з 3-х до 2-х.

Через те, що в даному випадку можна визначити тільки 2 параметри, третій параметр необхідно задати. Враховуючи те, що при проектуванні ТКС першочерговим є забезпечення параметра Pb, його необхідно прийняти заданим, згідно (4).

Отже, кількість варіантів необхідних для розгляду систем рівнянь зменшено з 60-и (рис.7) до 1-го.

На третьому етапі формується система 2-х рівнянь, необхідна для визначення 3-х параметрів. Особливістю такого формування є використання аналітичних залежностей для кожного з рівнянь в графічному виді. Далі розв'язок вказаної системи рівнянь здійснюється з використанням аналітично-графічного рішення системи рівнянь, що значно оптимізовує процес проектування певної ТКС.

Одним із рівнянь є залежність k (Eb/No), що приведена на рис.10. Вона використовується як «шаблон», перевагою якого є універсальність (останній не залежить від вимог до конкретної ТКС, зокрема до Ps). Для побудови залежності використано формулу Шеннона, модифіковану наступним чином [1] :

$$Eb/No = (2^{Cn} - 1)/Cn \quad . \qquad (12)$$

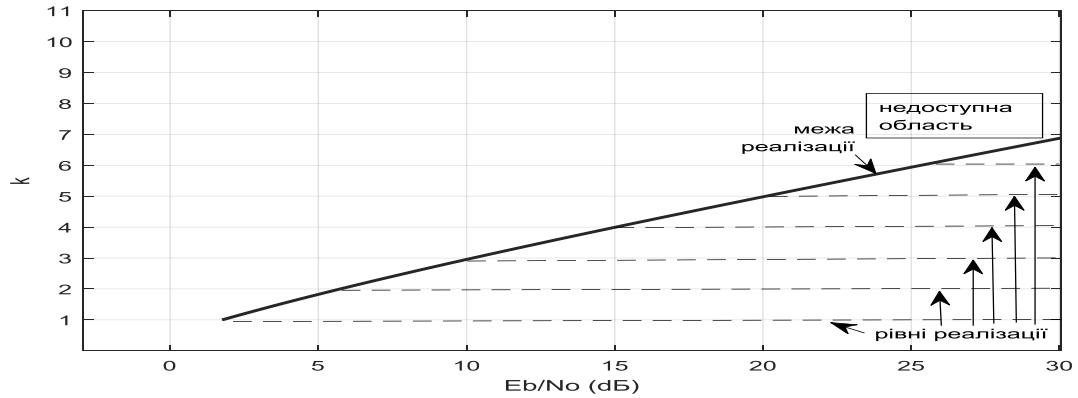


Рис.10. Залежність k(Eb/No)

Для отримання залежності k(Eb/No) в рівнянні (12) здійснено заміну Cn згідно (11).

При побудові графічних залежностей (рис.10 та інших) зручно використовувати значення параметра (Eb/No) в децибелах. Проте при визначенні Ps (5) застосовується відношення Eb/No (в разах). Для оперативного переходу між вказаними значеннями відношення сигнал/шум зручно мати таку можливість. Для цього пропонується використання суміщеного графіка (рис. 11), в якому відображаються дві функції спільного аргументу, але з суттєво різними значеннями по осі Y

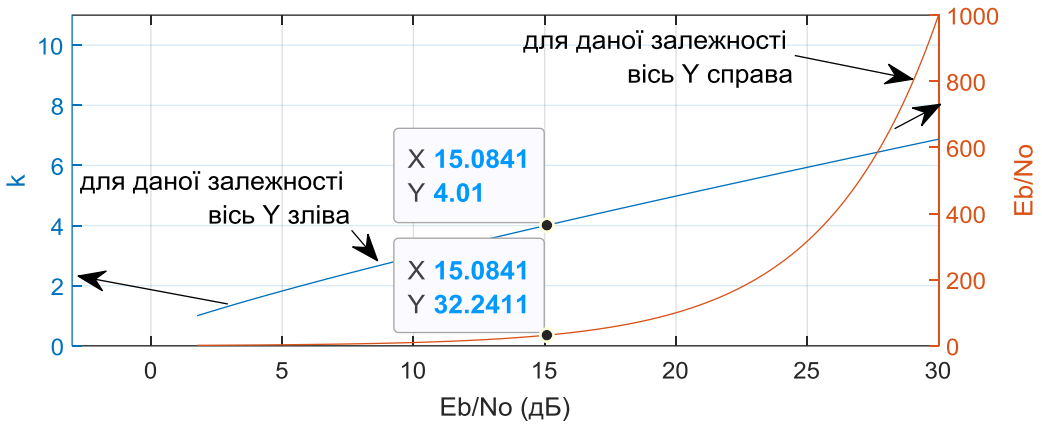


Рис.11. Суміщений графік для залежностей k(Eb/No, дБ) та Eb/No(Eb/No, дБ)

Видно, що для Eb/No = 15 дБ, значення Eb/No = 32.2

Другим рівнянням вказаної системи є залежність k (Eb/No) при значенні Pb = const, яке задається при проектуванні.

Проєктування при заданому значенні Ps **та вибір найбільш ефективної ТКС**

Таке проектування доцільно розглядати на прикладі конкретної ТКС (для якої Ps=Po=10^{-10}.

Для цього «шаблон» (рис.10) доповнюється залежністю k (Eb/No) при Ps = 10^{-10}, отриманої з використанням методу « 2D – 3D – 2D/ ».

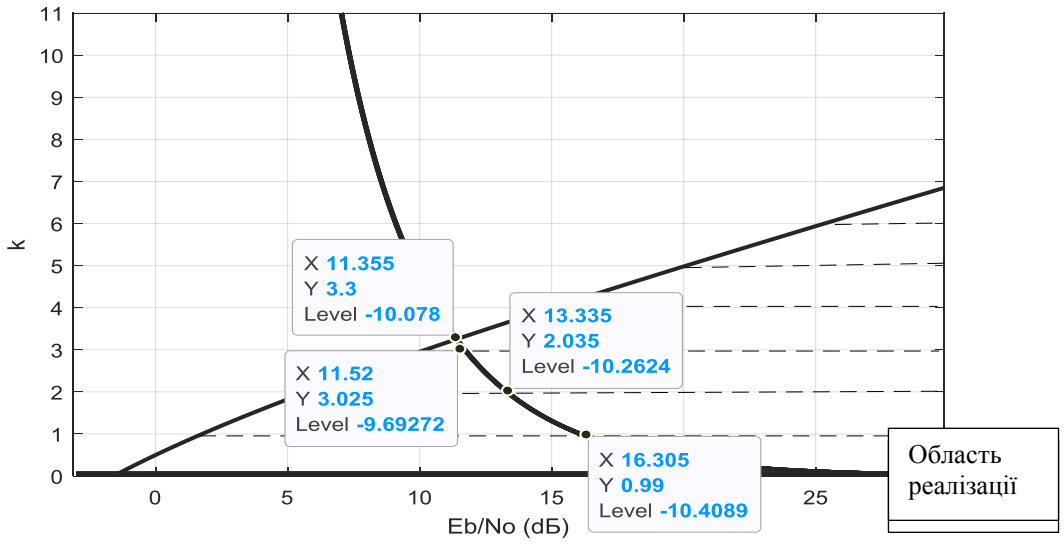


Рис.12. Визначення параметрів (k, Eb/No та Cn) ТКС при заданому значенні параметра Ps=Po=10^{-10}

Видно, що дана ТКС може бути реалізована при виконанні умови k ≤ 3.3. Враховуючи те, що параметр k може приймати тільки цілі значення, можливі 3 варіанти ефективних систем:

- при k=1 та Eb/No=16.3 дБ;
- при k=2 та Eb/No=13.3 дБ;
- при k=3 та Eb/No=11.5 дБ.

Звичайно, кожен із 3-х варіантів може реалізовуватися також при більшому значенні Eb/No (що небажано), тоді такий варіант перестає бути ефективним. Серед даних випадків найбільш ефективним є варіант при k=3, якому властиві суттєві переваги:

- необхідне найменше значення Eb/No=11.5 дБ;
- при більшому значенні k=3 забезпечується вище значення пропускної здатності C (11) навіть при W=const.

Таким чином для даної (найбільш ефективної) ТКС відомі вже 4 значення (заданий параметр $Ps=10^{-10}$, визначені параметри k=3, Eb/No=11.5 дБ та згідно (11) відношення C/W=2*3=6).

При цьому можливі два варіанти використання отриманої залежності C/W=2*3=6. Якщо відома наявна смуга частот, наприклад W=2 МГц, то отримується значення пропускної здатності C=2*6=12 Мбіт/с. Якщо ж задано необхідне значення пропускної здатності, наприклад 30 Мбіт/с, то необхідна смуга частот становить W = 30/6 = 5 МГц. Таким чином, отримано 5 параметрів даної ТКС.

Якщо необхідно отримати значення 6-го параметру (S/N, що потрібно не часто), то для цього використовуються залежності (2,б) та (11), що нескладно.

На основі наведеного прикладу розроблено алгоритм оптимального проектування ефективних ТКС (рис.13).

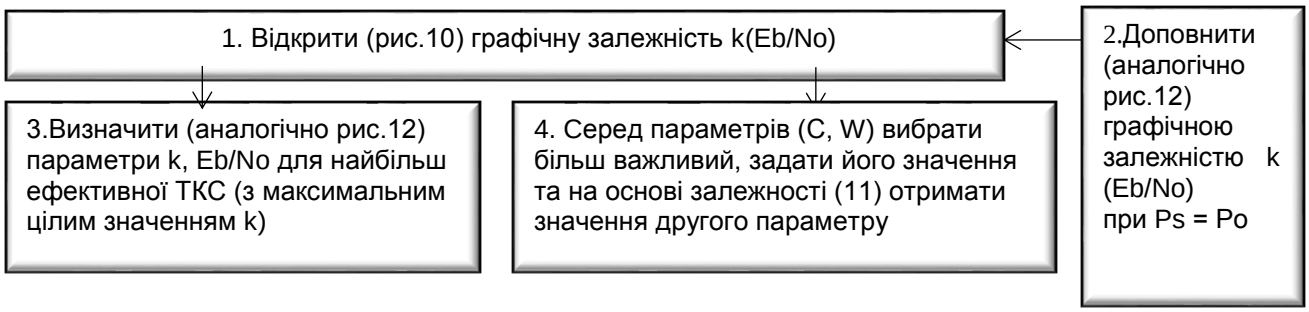


Рис.13. Алгоритм проектування ефективних ТКС

Висновки

В роботі розглянуто дві важливі складові, що стосуються реалізації ТКС: оптимізації проектування та вибору серед можливих варіантів реалізації ТКС більш ефективних.

1. Оптимізація проектування здійснюється завдяки широкому використанню сучасних програмних пакетів, зокрема MATLAB, що наближає проведене проектування до автоматизованого. Також широко використовується аналітично-графічний підхід, при якому складні (часто навіть неможливі) аналітичні перетворення замінюються еквівалентними графічними перетвореннями. При цьому процес проектування практично не ускладнюється, але забезпечує можливість візуального сприйняття суті обробки сигналів в окремих вузлах ТКС. Серед запропонованих шляхів оптимізації варто виділити наступні:

- визначення ймовірності помилкового приймання бітів інформаційних сигналів з допомогою спеціалізованих засобів пакету MATLAB;
- використання методу «2D- 3D- 2D/», що дозволяє спростити формування необхідних (для оптимізації проектування) графічних залежностей;
- застосування суміщених графіків, що дозволяють замінити необхідність незручного використання двох графічних вікон, зручністю використання одного графічного вікна.

2. На основі проведених досліджень розроблено алгоритм проектування ефективних ТКС, який дозволяє в кожному конкретному випадку:

- отримати всі можливі варіанти ефективних (згідно запропонованого критерію) ТКС;
- сформувати критерій вибору поміж отриманих варіантів більш ефективного.

Література

1.Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. Изд.2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс» , 2004. 1104 с.
2.Столлингс В.Беспроводные линии связи и сети. : Пер. с англ. М. : Издательский дом «Вильямс», 2003. 640 с. .
3.Сергиенко А.Б. Цифровая обработка сигналов: Учебник для вузов. 2-е изд. СПб.: Питер, 2007. 751 с.
4.. Климаш М.М, Пелішок В.О.. Проєектування ефективних систем бепровідного зв'язку. Digital signal processing. Modeling in MATLAB
Львів:, 2016. 232 с.
5.Солонина А.И., Арбузов С.М. Цифровая обработка сигналов. Моделирование в MATLAB. БХВ-Петербург, 2008. 816 с.
6.Дьяконов В.П. MATLAB SIMULINK для радиоинженеров. М.: ДМК Пресс, 2011. 976 с

References

1. Scliar, Bernard. Tsifrovaya sviaz. Teoreticheskiye osnovy i prcticheskoye primenieniye. Izd.2-ye, ispr.: Per. s angl.[Digital communication. Theoretical foundations and practical application]. M.: Izdatelskiy dom «Wiliams» , 2004. – 1104 s.
2. Stollings V. Besprovodnyye liniyi sviazi I sieti.[Wireless communication lines and networks.]. Per. s angl. - M. : Izdatelskiy dom «Wiliams», 2003. – 1104 s.: ил.
3. Sergiyenko A.B. Tsifrovaya obrabotka signalow: Uchebnik dlia vuzov [Digital signal processing]:. 2-ye izd. SPB.: Piter, 2007. 751 s.
4. Klymash. M.M.,. Pelishok V.O. Proektuvannia efektyvnyh system bezprovidnoho zviazku [Designing effective wireless communication systems]. Lviv: 2016. 232 s. Digital signal processing. Modeling in MATLAB
5. Solonina A.I., Arbuzov S.M. Tsifrovaya obrabotka signalow. Modelirovaniye v MATLAB[Digital signal processing. Modeling in MATLAB]. BXV-Peterburg, 2008. 816 s.
6. Diakonov V.P. MATLAB SIMULINK dlia radioinzhenierov.[MATLAB SIMULINK for radio engineers] M.: DMK PRESS, 2011. 976 sl.

УДК 004.942

ДОСЛІДЖЕННЯ СИСТЕМ МАСОВОГО ОБСЛУГОВУВАННЯ НА ОСНОВІ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ З УРАХУВАННЯМ МУЛЬТИАГЕНТНОГО ПІДХОДУ

DOI 10 36994 / 2788- 5518- 2022-02-04-12

Барабаш О.В., *д.т.н.,проф. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. bar64@ukr.net*

Колумбет В.П. *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. kvplinux@gmail.com*

Анотація: *Запропоновано предметно-орієнтований підхід до дослідження систем масового обслуговування (СМО). Прийняті рішення спрямовані на підвищення якості дій систем, поліпшення їх організації відповідно до прийнятого критерію якості роботи системи. У рамках цього підходу розробляються нові інтелектуальні моделі, алгоритми, методи та інструментарії, призначені для підтримки прийняття рішень у процесі управління системами масового обслуговування на базі структурного та параметричного аналізу їх характеристик, властивостей та процесів роботи. Це дозволить розширити діапазон досліджуваних умов функціонування інфраструктурних об'єктів, більш точно оцінити досягнуту ефективність функціонування СМО, заощадити ресурси, мінімізувати ризики помилок та збоїв.*

Ключові слова*: системи масового обслуговування, моделювання, інфраструктурні об'єкти, високопродуктивні обчислення*

RESEARCH OF MASS SERVICE SYSTEMS ON THE BASE OF SIMULATION MODELING TAKING INTO ACCOUNT THE MULTI-AGENT APPROACH

Oleg Barabash, *Dr. habil., Prof. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. bar64@ukr.net*

Vadym Kolumbet. *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. kvplinux@gmail.com*

Abstract*: Increasing the efficiency of managing complex objects is most often achieved by intellectualizing their control systems. In this regard, the article proposes a subject-oriented approach to the study of mass service systems (MSS). The number of questions that can be solved with the help of MSS analysis is endless and affects almost all areas of computer science and information technology. Being able to do this kind of analysis with this toolkit is important for those involved in these industries. The study of MSS provides an opportunity to obtain the necessary information and, thus, to prepare grounds for making decisions regarding the mode of operation of the system, improving its organization, etc. The adopted decisions are aimed at improving the quality of the systems' actions, improving their organization in accordance with the accepted criterion of the quality of the system's work. As part of this approach, new intelligent models, algorithms, methods and tools are developed, designed to support decision-making in the process of managing mass service systems based on structural and parametric analysis of their characteristics, properties and work processes. The listed developments are combined into a new specialized decision-making technology. The developed methods and tools for modeling mass service systems can be used in the process of researching various infrastructure objects. For this purpose, digital duplicates of infrastructure objects are being developed. They make it possible to expand the range of studied operating conditions of infrastructure objects. Their use makes it possible to more accurately assess the achieved efficiency of their creation and operation, save resources, minimize the risks of errors and equipment failures, extend the period of stable operation of these objects*

Key words: *mass service systems, modeling, infrastructure objects, high-performance computing.*

Вступ

В даний час дослідження поведінки складно організованих технічних систем масового обслуговування (СМО) на різних етапах їх проектування та функціонування є однією з важливих проблем імітаційного моделювання. Складність динамічної структури СМО обумовлена великою кількістю важливих характеристик функціонування СМО та зв'язків між ними, представлених

функціональними, статистичними, неоднозначними чи іншими відображеннями; існуванням широкого спектра випадкових подій та законів їх розподілу; наявністю обмежень різних видів [1].

СМО використовуються для моделювання процесів обслуговування клієнтів, виробництва, транспортування, зв'язку, обробки інформації, функціонування інфраструктурних об'єктів та інших процесів [2]. Застосування імітаційного моделювання дозволяє суттєво спростити розробку оптимальних режимів їх роботи, а також знаходження та вибір керуючих параметрів. У рамках такого моделювання розробляється імітаційна програма, що відтворює процеси роботи досліджуваної системи, визначаються її вхідні та вихідні параметри, задаються зовнішні дії. Підготовка багатоваріантних розрахунків здійснюється шляхом перебору значень вхідних змінних заданих діапазонах. До кожного варіанта вхідних змінних розраховуються відповідні вихідні змінні. Отримані результати розрахунків оптимізуються. Отже, оптимальні параметри процесів роботи системи обчислюються на основі методу грубої сили. Якість отриманих результатів моделювання багато в чому обумовлена ступенем повноти знань про предметну область досліджуваної системи, а також алгоритмів використовуваних під час вирішення завдань.

Імітаційне моделювання з урахуванням багатоваріантних розрахунків характеризується високою комбінаторною складністю. Це, у свою чергу, призводить до великих витрат оперативної пам'яті та дискового простору, а також значного навантаження на мережу. Тому для отримання якісних результатів моделювання СМО найчастіше потрібне застосування засобів високопродуктивних обчислень. Зазвичай такі кошти надаються центрами колективного використання (ЦКВ). В іншому випадку, необхідно спрощення моделі СМО, що зумовлює зниження якості результатів розв'язання задачі. Використання паралельних чи розподілених обчислень забезпечує підтримку проведення великомасштабних імітаційних експериментів, обробку вихідних даних більшого обсягу та розширення класу розв'язуваних завдань.

Необхідність урахування специфіки роботи СМО та аналізу інформаційних потоків даних актуалізує перехід від традиційної математичної моделі системи до її якісно нового вигляду – цифрового двійника, що містить актуальні дані про весь її життєвий цикл. В даний час такий перехід можливий завдяки стрімкому розвитку інформаційних технологій, збільшенню розмірів систем зберігання даних та суттєвому зростанню продуктивності обчислювальних систем, необхідному для обробки великих даних та ефективного отримання знань.

Цій тематиці було присвячено ряд сучасних робіт зарубіжних та вітчизняних вчених. Серед них зокрема варто виділити таких дослідників: Адамцев Д.Ю., Помазун О.М., Ланде Д.В., Страшной Л., Балагура І.В., Скулиш М.А. Аналіз наукових праць з імітаційного моделювання, методів підтримки прийняття рішень, мультиагентних підходів пов'язаних з темою дослідження, дозволяє зробити висновок, що користувачі можуть вибирати з доступних інструментів моделювання, які відрізняються точністю уявлення реального світу і ефективністю.

В роботі [3] розглядаються інструментальних засобів автоматизованого проектування комплексу технічних засобів інформаційної системи. Розкривається комплекс проблем, які виникають під час проектування комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Здійснено огляд загальних підходів до створення комплексних систем захисту інформації. Запропоновано загальний методологічний підхід до проектування систем захисту інформації в інформаційно-телекомунікаційних системах. Але, дані засоби та методи не враховують специфіку предметних областей досліджуваних систем.

В роботі [4] запропоновано методику формування, кластеризації, ранжирування та подальшої візуалізації спрямованих кореляційних мереж, зв’язки яких визначаються на основі рядів динаміки, що відповідають цим поняттям. Розглянуто часові ряди динаміки вживання термінів, що формуються сервісом Google Books Ngram Viewer для формування кореляційної мережі наукових понять, і часові ряди динаміки захворюваності на коронавірус у різних країнах для формування та кластеризації мережі країн за ознакою подібності відповідних статистичних рядів. Але, ця методика не повною мірою вирішує поставлене завдання та запропоновані інструментарії не повною мірою використовують доступні потужності обчислювального середовища.

В роботі [5] досліджувались процеси підтримки прийняття рішень у системі управління виробничо-збутовим процесом. Для багатокритеріальної оцінки варіантів з використанням апарату нечітких множин обрано вид функцій загальної корисності та корисності локальних критеріїв. Данна методика не повною мірою вирішує поставлене завдання, є

вузькоспеціалізованою та не має усіх необхідних функціональних можливостей для вирішення поставлених питань.

В статті [6] запропоновано систему підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки. Розроблено систему підтримки прийняття рішень, що дозволяє засобами системного підходу та ER-моделювання суттєво підвищити рівень інформаційної безпеки. Данна система не враховує специфіку предметних областей досліджуваних систем та запропоновані інструментарії не повною мірою використовують доступні потужності обчислювального середовища.

Отже, на підставі проведеного аналізу виявлено, що існуючі методи не повною мірою вирішують поставлене завдання та більшість інструментів не використовують доступні потужності обчислювального середовища та не враховують специфіку предметних областей досліджуваних систем, а також не забезпечують сервіс-орієнтований інтерфейс, що є важливим компонентом сучасних засобів моделювання.

Найчастіше відомі в даний час засоби імітаційного моделювання СМО у високопродуктивному обчислювальному середовищі або є вузькоспеціалізованими, які не мають усіх необхідних функціональних можливостей для вирішення зазначених вище проблем, або входять до складу дорогого програмного забезпечення і через це недоступні широкому колу кінцевих користувачів.

Виконання досліджень

Метою статті є запропонувати новий підхід до дослідження СМО, що базується на комплексному застосуванні методів концептуального програмування, інженерії знань, штучного інтелекту, багатокритеріальної оптимізації, паралельних та розподілених обчислень, віртуалізації ресурсів, а також мультиагентних та сервіс-орієнтованих технологій. Проаналізувати особливості зазначеного підходу та розробити практичні рекомендації щодо його застосування. Розглянуто архітектуру та принципи функціонування системи специфікації та моделювання процесів функціонування СМО.

Розробники програмного забезпечення для дослідження складних систем шляхом їх імітації відзначають такі його необхідні властивості, як підтримка часткової автоматизації складання моделей, їх верифікація та валідація, налаштування моделі на конкретну предметну область, реалізація комбінованого моделювання або гібридного моделювання, збір та обробка слабоструктурованих даних, їх реформування у структури, які використовуються моделлю, оптимізаційний аналіз результатів розрахунків.

Крім того, оскільки імітаційне моделювання веде до великих тимчасових та ресурсних витрат, потрібне використання високопродуктивної обчислювальної техніки, доступ до якої з боку користувачів має бути зручним та гнучким. Сервіс-орієнтована парадигма програмування дозволяє успішно реалізувати такий доступ.

Слід зазначити, що для ефективного проведення експериментів з імітаційними моделями у високопродуктивному обчислювальному середовищі має бути складена відповідна методика виконання досліджень.

Розглянута у статті технологія та моделювання процесів функціонування СМО повною мірою враховують вищезазначені вимоги. Дана методика виконання досліджень базується на спільному та узгодженому використанні методів автоматизації конструювання та застосування імітаційних моделей мовою GPSS на основі парадигм концептуального, модульного, каркасного та сервіс-орієнтованого програмування, інженерії знань, високопродуктивних обчислень та мультиагентних систем, а також методів аналізу експериментальних даних на основі дискретної багатокритеріальної оптимізації.

Цифровий двійник досліджуваної СМО базується на імітаційному моделюванні процесів її роботи за сукупністю ретроспективних та поточних даних. Цифрові двійники будуть використовуватись для розробки та налагодження нових стратегій управління СМО на основі оптимізаційного аналізу результатів багатоваріантних розрахунків [7]. Реалізація агентного моделювання у процесі дослідження реальної дозволить здійснювати верифікацію та валідацію імітаційної моделі шляхом напівнатурного моделювання.

В рамках агентного моделювання суб'єкти, пов'язані із забезпеченням експлуатації об'єкта та споживанням ресурсів і послуг наданих їм, делегують агентам свої права та обов'язки. Суб'єкти можуть задавати критерії ефективності функціонування об'єкта, які можуть бути

суперечливими. Агентний підхід дозволить враховувати та на основі багатокритеріальної оптимізації узгоджувати переваги суб'єктів, пов'язаних з об'єктом, у процесі його моделювання.

Багатоваріантні розрахунки виконуватимуться у обчислювальному середовищі, що об'єднує виділені та невиділені ресурси. Для керування виділеними ресурсами обрано програмний комплекс OpenStack, який забезпечує взаємодію з різними гіпервізорами (KVM, Xen, QEMU та ін.), а також із системами керування контейнерами (Docker та ін.). На базі цього комплексу створено новий менеджер віртуальних машин. Цей менеджер підтримує можливість запуску завдань із виконання віртуальних машин із загальних черг (наприклад, PBS, SLURM) на невиділених ресурсах суперкомп'ютерів ЦКВ [9]. Віртуальні машини, запущені на виділених та невиділених ресурсах для прогону екземплярів моделі в паралельному режимі, підключатимуться до єдиного віртуалізованого середовища, організованого на основі технології Virtual Private Network (VPN).

Елементарні функціональні можливості цифрових двійників та агентів будуть представлені у вигляді мікросервісів. Такий підхід дозволить організувати взаємодію між вищезгаданими віртуальними сутностями на базі ефективних мережевих протоколів та спростить процеси додавання нових та модифікацію існуючих двійників та агентів. Залишаються незрозумілими відповіді на конкретні питання, що саме треба зробити - збільшувати кількість каналів або збільшувати їхню пропускну здатність, або збільшувати кількість місць у черзі? Щоб оцінити чутливість кожного показника до зміни значення певного параметра, використовуємо такий підхід: фіксуємо всі параметри крім одного, обраного. Потім знімаємо значення всіх показників при декількох значеннях цього обраного параметра. Звичайно, доводиться повторювати знову й знову процедуру імітації й усереднювати показники при кожнім значенні параметра, оцінювати точність. Але в результаті виходять надійні статистичні залежності показників від параметра [10]. Наприклад, для 6 показників можна одержати 6 залежностей від одного параметра: залежність імовірності відмов $P_{\text{відм.}}$ від кількості місць у черзі (СМО), залежність пропускної здатності A від кількості місць у черзі, і так далі [12]. Залежність показників від параметрів СМО відображено на рис. 1.

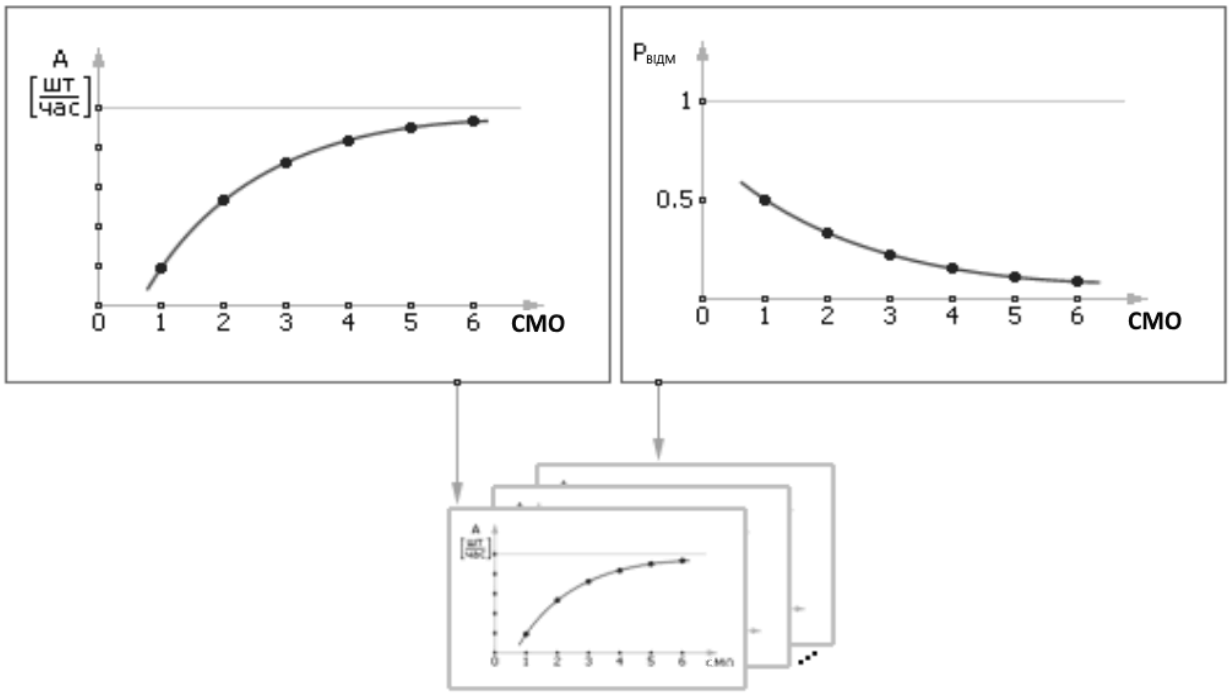


Рис. 1. Залежність показників від параметрів СМО

Потім так само можна зняти ще 6 залежностей показників P від іншого параметра R, зафіксувавши інші параметри і так далі. Утвориться своєрідна матриця залежностей показників P від параметрів R, по якій можна провести додатковий аналіз про перспективи поліпшення показників у ту або іншу сторону. Нахил кривих добре показує чутливість, ефект від руху по

певному показнику. Таку матрицю називають якобіаном J, у якій роль нахилу кривих грають значення похідних $\Delta P_i / \Delta R_j$ (рис. 2).

Якщо показників 6, а параметрів, наприклад, 5, то матриця має розмірність 6 х 5. Кожен елемент матриці - крива, залежність $i-$ го показника від $j-$ го параметра. Кожна крапка кривої - середнє значення показника на досить представницькому відрізку Тн або усереднено по декількох експериментах. Варто розуміти, що криві знімалися в припущенні того, що всі параметри крім одного в процесі їхнього зняття були незмінні. Тому, якщо на підставі розгляду знятих кривих приймається рішення про те, що деякий параметр буде в СМО змінений, те всі криві для нової крапки, у якій знову буде досліджуватися питання про те, який параметр варто змінити, щоб поліпшити показники, варто знімати заново. Так крок за кроком можна спробувати поліпшити якість системи.

$$\|J\| = \begin{vmatrix} J_{11} & J_{12} & J_{13} & \dots & J_{1,6} \\ J_{21} & J_{22} & J_{23} & \dots & J_{2,6} \\ \dots & \dots & \dots & \dots & \dots \\ J_{51} & J_{52} & J_{53} & \dots & J_{5,6} \end{vmatrix} = \begin{vmatrix} \frac{\Delta P_1}{\Delta R_1} & \frac{\Delta P_1}{\Delta R_2} & \frac{\Delta P_1}{\Delta R_3} & \dots & \frac{\Delta P_1}{\Delta R_6} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{\Delta P_5}{\Delta R_1} & \frac{\Delta P_5}{\Delta R_2} & \frac{\Delta P_5}{\Delta R_3} & \dots & \frac{\Delta P_5}{\Delta R_6} \end{vmatrix} =$$

$$= \left| \begin{array}{ccc} \text{A} & \text{P}_{\text{відм.}} & \\ J_5 \quad \text{СМО} & J_6 \quad \text{СМО} & \dots \\ \dots & \dots & \\ & & \end{array} \right|_{6 \text{ x } 5}$$

Рис. 2. Матриця чутливостей показників залежно від зміни параметрів СМО

Для доступу до розроблених засобів у процесі підготовки та проведення експериментів кінцеві користувачі будуть забезпечені веб-орієнтованим інтерфейсом [13]. До таких осіб можна віднести: різних категорій: розробники програмного забезпечення, адміністратори інформаційно-обчислювальних ресурсів, експерти з прийняття рішень щодо оптимізації функціонування інфраструктурних об'єктів на основі результатів їх моделювання та інші особи. Оптимізаційна постановка завдання у рамках такого дослідження наведена нижче.

Нехай $x = (x_1 1, x_2, \dots, x_c)$ – це вектор економічних показників споживання ресурсів (електроспоживання, теплопостачання, споживання води тощо) у процесі експлуатації інфраструктурного об'єкта у період τ. Стан технічних, що використовуються об'єктом, представлено вектором $b = (b_1, b_2, \dots, b_v)$ булевих змінних. Елемент $b_i = 0$ $(b_1 = 1)$ означає, що $i-$ й пристрій виключено (включено), $i \in 1, l$.

Характеристики пристроїв представлені множиною параметрів $C = \{c_1, c_2, \dots, c_h\}$. На множині C визначено множину операцій $F = \{f_1, f_2, \dots, f_w\}$. Операція f $\in F$ забезпечує розрахунок необхідних цільових параметрів C за початковими даними, також представлених параметрами C.

Виділимо у множині C підмножини параметрів, що відображають експлуатаційні показники та керуючі параметри об'єкта. Ці підмножини параметрів представимо векторами $q = (q_1, q_2, \dots, q_p)$ та $u = (u_1, u_2, \dots, u_r)$.

Поточні показники довкілля об'єкта відображені речовою матрицею O розмірності $m \times n$. Елемент матриці o_{ij} містить значення $i-$го показника в j годину періоду τ. Ретроспективні показники навколишнього середовища аналогічно представлені речовою матрицею Y такої ж розмірності.

Відобразимо цільову функцію у такому вигляді:

$$y\,(x\,,\tau,O,Y,b\,v)\;=\sum_{i-1}^{n}x_i\;\rightarrow\;min,$$
$$h_j\,(b)=\;0,q_s\;\rightarrow\;min\,(max),$$
$$q_s^{min}\;\leq q_s\leq\;q_s^{max}\,,s\;=\overline{1,p}\,,$$

де $h_1(b), h_2 2(b), \ldots, h_o(b)$ – це булеві функції, що накладають обмеження на спільне використання технічних пристроїв, $q_s \rightarrow min(max)$ – умова оптимальності $s-$го експлуатаційного показника, q_s^{min} та q_s^{max} – його граничні значення, $v = (v_1, v_2, \ldots, v_z)$ - Вектор вхідних параметрів моделі, $v_t \in C, t = 1, z$.

Збір, уніфікацію, агрегування, зберігання та передачу даних про роботу інфраструктурного об'єкта здійснюватиме спеціальна система моніторингу інформаційно-обчислювальних систем, адаптована до обслуговування об'єктів даного виду.

Визначення оптимальних значень експлуатаційних показників здійснюється шляхом прогону екземплярів моделі з різними варіантами її вхідних параметрів з подальшим застосуванням правил дискретного багатокритеріального вибору [14]. Якщо оптимальному варіанту експлуатаційних показників відповідає кілька варіантів вхідних змінних моделі, то вибір оптимального варіанту проводиться за допомогою тих самих правил.

Висновки

Запропоновано новий підхід до дослідження СМО, що базується на комплексному застосуванні методів концептуального програмування, інженерії знань, штучного інтелекту, багатокритеріальної оптимізації, паралельних та розподілених обчислень, віртуалізації ресурсів, а також мультиагентних та сервіс-орієнтованих технологій. Проаналізовано особливості зазначеного підходу та розроблено практичні рекомендації щодо його застосування. Проведено дослідження можливості створення моделей, алгоритмів, методів та інструментів, призначених для інтелектуальної підтримки прийняття рішень у процесі управління СМО на базі структурного та параметричного аналізу їх характеристик, властивостей та процесів роботи. На основі результатів дослідження показано нову модель підтримки прийняття рішень, що базується на багатокритеріальному аналізі результатів імітації роботи досліджуваних систем у обчислювальному середовищі, яка складається з різнорідних високопродуктивних ресурсів. Таке середовище може містити ресурси центрів колективного користування, включаючи суперкомп'ютери. Представлені методи та засоби моделювання СМО можуть бути застосовані у процесі дослідження інфраструктурних об'єктів, що, у свою чергу, дозволить суттєво покращити економічні показники функціонування досліджуваних об'єктів.

Література

1. Uhlemann T.H.-J., Lehmann C., Steinhilper R. The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0. *Procedia CIRP*. 2017. Vol. 61. P. 335–340. doi:10.1016/ j.procir.2016.11.152

2. Омельяненко В.А. Мультиагентний підхід до розробки інтелектуальних систем управління проектами. *Управління проектами та розвиток виробництва*, 2016. № 3 (59). С. 5–13.

3. Кобозєва А.А. Розробка інструментальних засобів автоматизованого проектування комплексу технічних засобів інформаційної системи. *Кібербезпека в Україні: правові та організаційні питання*. Матеріали міжнародної науково-практичної конференції, 26 листопада 2020 р. Одеса. 2021. С. 86–89.

4. Ланде Д.В., Страшной Л., Балагура І.В. Метод формування та кластеризації кореляційних мереж понять. *Реєстрація, зберігання і обробка даних*, 2021, Т. 23, № 2. С. 27–36.

5. Адамцев Д.Ю., Прокопенко Д.І. Підтримка прийняття рішень у системі управління виробничо-збутовим процесом. *Automation and development of electronic devices*, 2021, Part 2. С. 139–143.

6. Азарова А., Дьогтєва І., Шиян А. Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. *Інформаційні технології та комп'ютерна інженерія*, 2022. Вип. 53, № 1. С. 12–18.

7. Скулиш М.А. Математична модель пошуку оптимального обсягу ресурсів віртуального вузла обслуговування. *Сучасні інформаційні системи*, 2018. Том 2, № 2. С. 30-34. doi: 10.20998/2522-9052.2018.2.05

8. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine. 2018. Vol. 51. № 11. P. 1016–1022. doi: 10.1016/j.ifacol.2018.08.474.
9. Касілов О.В., Крамська К.І. Моделі і метод синтезу агентної інформаційно-пошукової системи. *Сучасні інформаційні системи*. 2020. Т. 4, № 2. С. 94–99. doi:10.20998/2522-9052.2020.2.14
10. Iafrate F. A Journey from Big Data to Smart Data. Proceedings of the Second International Conference on Digital Enterprise Design and Management. Springer, Cham, 2014. P. 25–33. doi: 10.1007/978-3-319-04313-5_3.
11. Kolumbet, V., Svynchuk, O. Multiagent methods of management of distributed computing in hybrid clusters. Сучасні інформаційні системи. 2022. Т. 6, № 1. С. 32–36. doi:10.20998/2522-9052.2022.1.05
12. Додонов О.Г., Коваль О.В., Сенченко В.Р., Шпурик В.В. Автоматизована система формування сценарію аналітичної діяльності. *Реєстрація, зберігання і обробка даних*, 2019, Т. 21, № 1. С. 11–22.
13. Помазун О.М. Особливості побудови групової системи підтримки прийняття рішень з реінжинірингу бізнес-процесів. *Вісник Запорізького національного університету*, 2009, № 1 (4). С. 83–88.
14. Кучук Г.А., Коваленко А.А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. *Сучасні інформаційні системи*, 2018. Том 2, № 1. С. 22–27. doi: 10.20998/2522-9052.2018.1.04

References

1. Uhlemann T.H.-J., Lehmann C., Steinhilper R. The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0. *Procedia CIRP*. 2017. Vol. 61. P. 335–340. doi:10.1016/ j.procir.2016.11.152
2. Omelyanenko V.A. Multiagentnij pidhid do rozrobki intelektualnih sistem upravlinnya proektami. [A multi-agent approach to the development of intelligent project management systems]. *Upravlinnya proektami ta rozvitok virobnictva*, 2016. № 3 (59). pp. 5–13. [in Ukrainian].
3. Kobozyeva A.A. Rozrobka instrumentalnih zasobiv avtomatizovanogo proektuvannya kompleksu tehnichnih zasobiv informacijnoyi sistemi. [Development of tools for automated design of a complex of technical means of the information system]. *Kiberbezpeka v Ukrayini: pravovi ta organizacijni pitannya*. Materiali mizhnarodnoyi naukovo-praktichnoyi konferenciyi, 26 listopada 2020. Odesa. 2021. pp. 86–89. [in Ukrainian].
4. Lande D.V., Strashnoj L., Balagura I.V. Metod formuvannya ta klasterizaciyi korelyacijnih merezh ponyat. [Method of formation and clustering of correlation networks of concepts. Registration, storage and processing of data]. *Reyestraciya, zberigannya i obrobka danih*, 2021, Vol. 23, № 2. pp. 27–36. [in Ukrainian].
5. Adamcev D.Yu., Prokopenko D.I. Pidtrimka prijnyattya rishen u sistemi upravlinnya virobnicho-zbutovim procesom. [Decision-making support in the production and sales process management system]. *Automation and development of electronic devices*, 2021, Part 2. pp. 139–143. [in Ukrainian].
6. Azarova A., Dogtyeva I., Shiyan A. Sistema pidtrimki prijnyattya rishen shodo pidvishennya rivnya informacijnoyi bezpeki pidpriyemstva. [Decision support system for increasing the level of information security of the enterprise]. *Informacijni tehnologiyi ta komp'yuterna inzheneriya*, 2022. Vol. 53, № 1. pp. 12–18. [in Ukrainian].
7. Skulish M. A. Matematichna model poshuku optimalnogo obsyagu resursiv virtualnogo vuzla obslugovuvannya. [Mathematical model of finding the optimal amount of resources of a virtual service node]. *Suchasni informacijni sistemi*, 2018. Vol. 2, № 2. pp. 30–34. doi: 10.20998/2522-9052.2018.2.05 [in Ukrainian].
8. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine. 2018. Vol. 51. № 11. P. 1016–1022. doi: 10.1016/j.ifacol.2018.08.474.
9. Kasilov O.V., Kramska K.I. Modeli i metod sintezu agentnoyi informacijno-poshukovoyi sistemi. [Models and method of synthesis of agent information and search system]. *Suchasni informacijni sistemi*. 2020. Vol. 4, № 2. pp. 94–99. doi:10.20998/2522-9052.2020.2.14 [in Ukrainian].
10. Iafrate F. A Journey from Big Data to Smart Data. Proceedings of the Second International Conference on Digital Enterprise Design and Management. Springer, Cham, 2014. P. 25–33. doi: 10.1007/978-3-319-04313-5_3.
11. Kolumbet, V., Svynchuk, O. Multiagent methods of management of distributed computing in hybrid clusters. Advanced Information Systems. 2022. Vol. 6, № 1. pp. 32–36. doi:10.20998/2522-9052.2022.1.05 [in English].
12. Dodonov O.G., Koval O.V., Senchenko V.R., Shpurik V.V. Avtomatizovana sistema formuvannya scenariyu analitichnoyi diyalnosti. [Automated system for creating a scenario of analytical activity]. Reyestraciya, zberigannya i obrobka danih, 2019, Vol. 21, № 1. pp. 11–22. [in Ukrainian].
13. Pomazun O.M. Osoblivosti pobudovi grupovoyi sistemi pidtrimki prijnyattya rishen z reinzhiniringu biznes-procesiv. [Peculiarities of building a group decision support system for business process reengineering]. *Visnik Zaporizkogo nacionalnogo universitetu*, 2009, № 1 (4). pp. 83–88. [in Ukrainian].
14. Kuchuk G.A., Kovalenko A.A. Metodi sintezu informacijnoyi ta tehnichnoyi struktur sistemi upravlinnya ob'yektom kritichnogo zastosuvannya. [Methods of synthesizing the information and technical structures of the critical application facility management system]. *Suchasni informacijni sistemi*, 2018. Vol. 2, № 1. pp. 22–27. doi: 10.20998/2522-9052.2018.1.04 [in Ukrainian].

УДК 004.8

ПЕРСОНАЛІЗОВАНЕ НАДСИЛАННЯ СПОВІЩЕНЬ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

DOI 10 36994 / 2788- 5518- 2022-02-04-13

Матвієнко Н.Т. *Національний технічний університет України «Київський політехнічний Інститут імені Ігоря Сікорського», Київ, Україна. matvienkont@yahoo.com*

Могильний С.Б., *к.т.н. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. isearch@ukr.net*

Рожаловець К.*С. Відкритий міжнародний університет розвитку людини «Україна», Київ,Україна. konstantin.rozaholavets@gmail.com*

Анотація: *Метою цієї статті є дослідити та спрогнозувати етапи та шляхи розвитку інфраструктури для баз даних фінансових установ, що пов'язані із індустріальними регуляціями. Розглянуто основні тенденції в IT в цілому та у вибраному домені, наведені порівняльні розрахунки для безсерверних хмарних сервісів та самоінстальованих баз даних.*

Ключові слова: *бази данних, AWS, публічна хмара, безсерверні технології, RDS, EC2, фінансовий сектор.*

SENDING PERSONALIZED USER NOTIFICATIONS POWERED BY MACHINE LEARNING

Nazar Matviienko. *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukrain. matvienkont@yahoo.com*

Sergij Mohylnyy, *Ph.D. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",Kyiv, Ukraine. isearch@ukr.net*

Konstantyn Rozhalovets. *Open International University of Human Development "Ukraine",Kyiv, Ukraine. rozaholavets@gmail.com*

Abstract*: The article deals with the system of sending notifications to users. It is proposed to create a notification scheduling algorithm using deep learning, which includes: a data processing algorithm for training and the construction of a long-short-term memory (LSTM) network model that performs the scheduling most efficiently. The algorithm allows to improve the effectiveness of notifications through personalization, taking into account the gender, age and previous history of the target object.*

One of the most important indicators of the notification system in the information and telecommunication system (ITS) is the timeliness of sending notifications to the target object, which is a dynamic variable in the system. This indicator of timeliness cannot be calculated absolutely precisely, since it has a large number of dependencies that cannot be tracked absolutely accurately.

The proposed model offers a technique to create personalized notifications to increase timeliness by considering gender, age, and previous activity history.The result of more accurate planning of notifications is an increase in the effectiveness of feedback, which increases the amount of time the user spends on a resource that provides services in one or another area, which is the main reason for the existence of a notification system. The improved scheduling system can be applied in many areas with high traffic: web services for educators and students, news/magazine portals, video hosting, online marketing, entertainment services and other areas.

For planning in the notification system, it is proposed to use LSTM recurrent neural network in combination with elements of feed forward neural network. An LSTM network is able to store its input data in internal memory, which plays a key and integral role in solving problems involving sequential data.

Key words: *information and telecommunication system, notification system, machine learning, personalized notifications.*

Вступ

Одним з найголовніших показників системи сповіщень в інформаційно-телекомунікаційній системі (ІКТС) є своєчасність відправки сповіщень цільовому об'єкту, що є динамічною змінною в системі. Даний показник своєчасності неможливо порахувати абсолютно точно, оскільки він має в собі велику кількість залежностей, які не можна відслідкувати достеменно.

Запропонована модель пропонує методику для створення персоніфікованих сповіщень, щоб збільшити показник своєчасності шляхом врахування статі, віку та попередньої історії активності. Оскільки дані параметри властиві всім користувачам ІКТС, вони дають змогу знайти схожі патерни активності, що дає цінну інформацію для планування надсилання сповіщень вчасно.

Результатом більш точнішого планування сповіщень є збільшення ефективності відгуків, що збільшує кількість часу користувач проводить на ресурсі, що надає послуги в тій чи іншій сфері, що є найголовнішою причиною існування системи сповіщення. Покращену систему планування можна за стосувати в багатьох сферах з великим трафіком: веб-сервіси для освітян, портали новин/журналів, відеохостинги, онлайн-маркетинг, сервіси розваг та інші сфери.

Виконання досліджень

У статті буде використано анонімна база даних з інтернет-ресурсу, який надає послуги з навчання освітян на різні тематики. Особливістю алгоритму те, що таку базу даних можна зібрати для кожної ІКТС окремо, оскільки необхідні дані зазвичай присутні в системі логування та інформації користувача, при цьому дотримуючись приватності цих користувачів через узагальненість таких даних. В результаті обробки та очистки, вигляд даних на вхід навчальної моделі буде мати наступний вигляд:

$$\{ s, a, t1, t2, t3, t4, t5, t6, t7, t8, t9 \}, \quad (1)$$

де s — стать користувача,
a — вік користувача,
t1,...,t9 — часові мітки останньої активності користувача в послідовному порядку.

Експериментальним шляхом було прийдено до рішення вибрати 9 часових міток останньої активності, а на виході надавати 3 обраховані часові мітки наступного вигляду:

$$\{ p1, p2, p3 \}, \quad (2)$$

де p1, p2, p3 — обраховані часові мітки моделлю.

Змінні t1,...,t9 обробляються таким чином, щоб кожне з цих значень представляло рівно 1 годину на проміжку 1 рік (представлений датасет в статті дозволяє взяти такий проміжок) за формулою 2 для кожного значення:

$$(\text{TIMESTAMP} - \text{START\_OF\_YEAR})//\text{ONE\_HOUR},$$

де TIMESTAMP — одинарна мітка часу (Unix стандарт) активності користувача,
START_OF_YEAR - початок року в рік одинарної мітки TIMESTAMP,
ONE_HOUR — 3600 секунд в одній годині,
// — ділення з остачею.

Наприклад, TIMESTAMP = 1480453179 (Tuesday, November 29, 2016 20:59:39 UTC), START_OF_YEAR = 1451606400 (Friday, January 1, 2016 0:00:00 UTC). Звідси, перетворене число для навчання буде рівне 3579. Дане форматування має такі переваги:

- Модель навчання працює з невеликим числами, що зменшує навантаження на навчання, прискорюючи роботу;
- Дає змогу робити планування маючи активності користувачів наступних років, а не тільки обмежується роком коли навчали модель.

Недоліком є ускладнене планування на перехідному періоді між роками, проте її можна уникнути якщо взяти базу даних з даними більше 1 року.

Для планування в системі сповіщень пропонується використовувати LSTM рекурентну нейронну мережу в комбінації з елементом нейронної мережі прямого поширення. Мережа LSTM має змогу пам'ятати свої вхідні дані у внутрішній пам'яті, що відіграє ключову та невід'ємну роль у вирішенні проблем, що пов'язані з послідовними даними. Тому рекурентні мережам віддається перевага як алгоритму для послідовних даних: часових рядів, розпізнавання мови, тексту фінансові дані, аудіо- та відеоряди, погода та інші типи даних. LSTM мережа виділяється серед конкурентів точнішим вивченням важливих залежностей, які маю більшу відстань один від одного. Обрана мережа здатні охоплювати складніші задачі, використовуючи її ключові елементи для контролю попередніх даних для наступних значень, що називаються затвори.

Ключовим компонентом LSTM є стан елементу, що є горизонтальною шиною, що проходить через весь нейрон. Тому ця мережа здатна віднімати або додавати інформацію зі стану елемента шляхом відрегульованих структур – затворами:

- Затвор забуття – вирішує яку інформацію потрібно видалити з стану елементу;
- Затвор оновлення – сукупність двох функцій, використана для оновлення загального стану елементу;
- Вихідний затвор – сукупність функцій, що вирішують які дані будуть передані на вихід.

Експериментальним шляхом було знайдено оптимальну структуру моделі, яка забезпечує високу швидкість навчання та найкращу точність знаходження наступних часових міток на оціночних даних.

```
Model: "sequential_8"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 bidirectional_8 (Bidirectio  (None, 40)               3840
 nal)

 dense_16 (Dense)            (None, 50)                2050

 dense_17 (Dense)            (None, 3)                 153

=================================================================
Total params: 6,043
Trainable params: 6,043
Non-trainable params: 0
```

Рис. 1. Структура побудованої нейронної мережі

З структури бачимо, що двонаправленому режимі вхідні дані проходять у двох напрямках, що робить BiLSTM відмінним від звичайної LSTM. При глибокому навчанні модель повинна підібрати 6043 параметри, щоб робити ефективні обрахування для різних потоків даних, які не пов’язані один з одним.

Було здійснено процес навчання, який зайняв 64 хвилини, навчившись на 825 000 різних мультизмінних послідовностях. В результаті навчання на тренувальних даних було зроблено оцінку точності планування провівши 21000 прогнозувань, вхідними даними яких при цьому було використано тестувальні дані приведені в аналогічний формат, результати яких зображено на рис. 2.

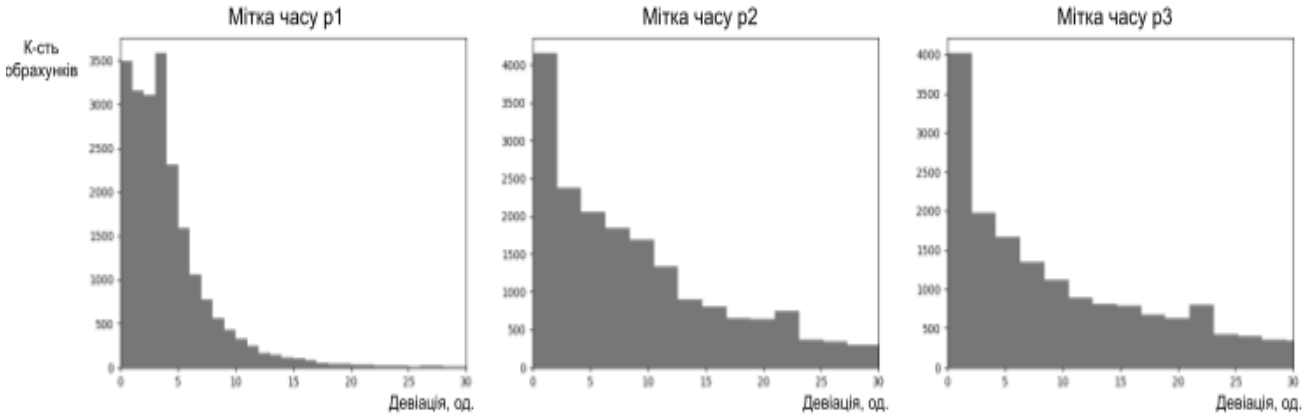


Рис. 2. Девіація мультикрокового прогнозування для 500 випадкових користувачів

З графіків видно, що більша частина обрахунків припадає на незначну девіацію в часі. В першому кроці обрахунку припадає 80% прогнозованих результатів з 23600 на девіацію 0-5 годин відносно зарані відомої правильної відповіді.

В табл.1 наведені статистичні значення прогнозувань для першого кроку.

Таблиця 1.

Статистичні значення прогнозувань для першого кроку

Девіація, год	0	1	2	3	4	5	6	7	8	9	10
К-ість прогнозувань	4018	7533	11027	15090	17541	19096	20155	20919	21459	21854	22157
Всього прогнозувань	23600	23600	23600	23600	23600	23600	23600	23600	23600	23600	23600
Частка з включно попередніми девіаціями, %	17,03	31,92	46,72	63,94	74,33	80,92	85,40	88,64	90,93	92,60	93,89

Значення з табл. 1 вказують на те, що побудована система сповіщень у 80% випадках правильно прогнозує наступний вхід користувача в систему.

Таблиця 2.

Статистичні значення прогнозувань для другого кроку

Девіація, год	0	1	2	3	4	5	6	7	8	9	10
К-ість прогнозувань	1915	3592	4999	6409	7791	9020	10123	11103	12066	12943	13858
Всього прогнозувань	23580	23580	23580	23580	23580	23580	23580	23580	23580	23580	23580
Частка з включно попередніми девіаціями, %	8.12	15.23	21.20	27.18	33.04	38.25	42.93	47.09	51.17	54.89	58.77

В табл. 2 зображена девіація для другого кроку прогнозувань, звідки видно, що відсоток спадає до 38% точності.

Табл. 3 показує, що девіація зростає, а її відсоткове відношення при девіації 0-5 годин сягає 30%. З цього можна зробити висновок, що найбільша точність отримується при першому кроці, а точність другого та третього – зменшується.

Таблиця 3

. Статистичні значення прогнозувань для третього кроку

Девіація, год	1	2	3	4	5	6	7	8	9	10	11
К-ість прогнозувань	1828	3472	4860	6084	7150	8150	9019	9742	10399	11001	11606
Всього прогнозувань	23318	23318	23318	23318	23318	23318	23318	23318	23318	23318	23318
Частка з включно попередніми девіаціями, %	7.84	14.89	20.84	26.09	30.66	34.95	38.68	41.78	44.60	47.18	49.77

Для оцінки впливу даних на роботу моделі було погруповано дані по даті народження – 1970-1975, 1985-1990, 1990-1995. При цьому графік розподілу кількості навчальних даних по віку зображено на рис. 3, що вказує на те що основна маса даних припадає на користувачів 1990-1995 року народження

.

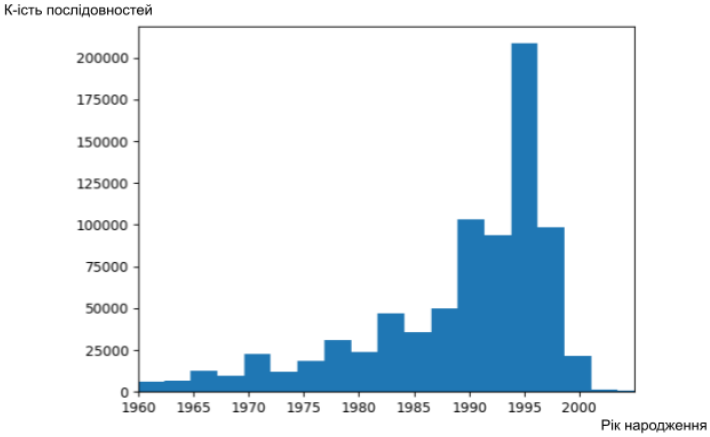


Рис. 3. Розподіл даних за роком народження

На рис. 4 зображено прогнозування для випадкових користувачів 1970-1975 року з даних для тестування.

Згідно рис. 4, для першого кроку прогнозування значення сума охоплених результатів з девіацією 0-5 рівна 77%, для другого – 38%, для третього – 30%.

Графік рис. 5 показує, що для першого кроку прогнозування значення сума охоплених результатів з девіацією 0-5 рівна 84%, для другого – 41%, для третього – 38%.

На рис.6 наведені дані прогнозування для користувачів 1990-1995 року.

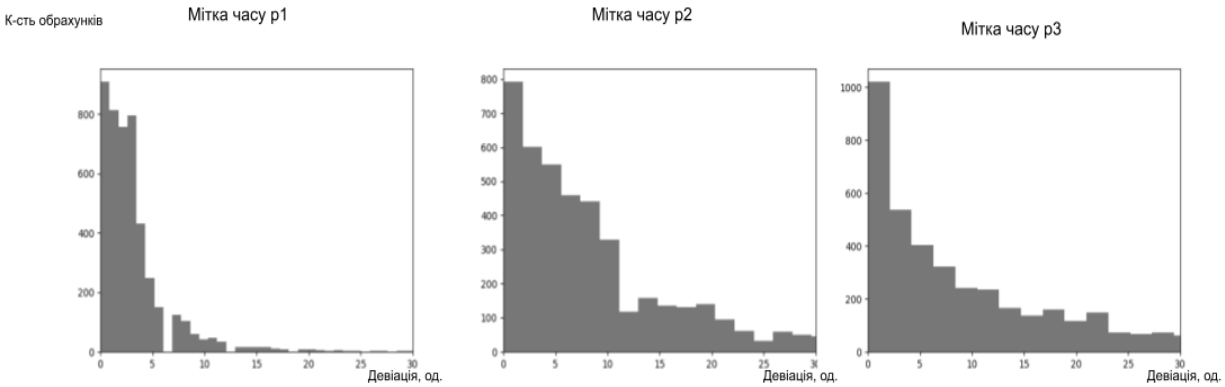


Рис. 4. Прогнозування для користувачів 1985-1990 року

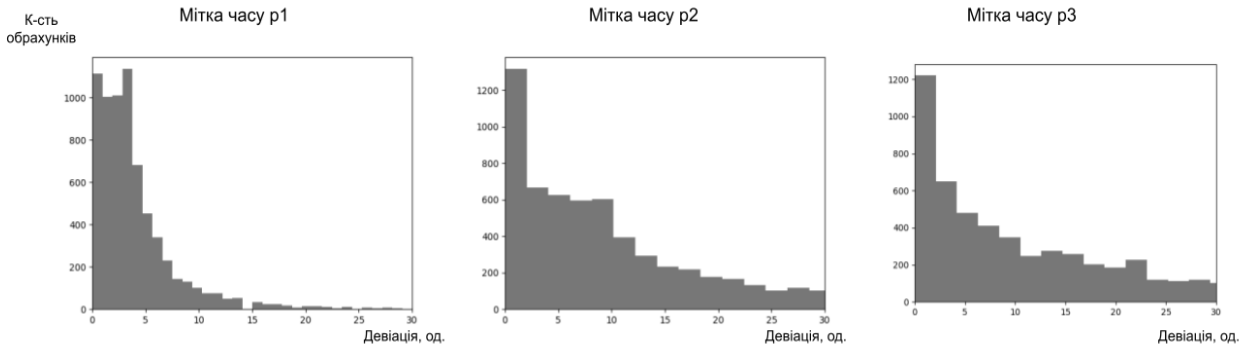


Рис.5. Прогнозування для користувачів 1990-1995 року

З рис. 6, для першого кроку прогнозування значення сума охоплених результатів з девіацією 0-5 рівна 79%, для другого – 33%, для третього – 31%. Що показує, що для даних 1990-1995 року результати прогнозування приблизно такі ж самі як і для даних 1970-1975. Але варто зауважити,

згідно графіку розподілу даних за роком народження, що дані 1990-1995 року мають в 20 разів більший об'єм, ніж дані 1970-1975 року. Схожі результати вказують на те, що модель з використанням LSTM нейронної мережі здатна адаптуватися до складних даних з великою кількістю варіативністю, даючи гнучкість системі для мультизмінних послідовностей, що відрізняються один від одного.

Висновки

1. Завдяки глибокому навчанню було створено методику планування системи сповіщень з метою підвищення своєчасності їх надсилання.
2. Робота пропонує метод врахування персоналізації на базі існуючих знань про стать, вік та історію активності користувачів.
3. Вихідний алгоритм крім гнучкості в персоніфікації пропонує також мультикрокове планування сповіщень.
4. Експериментальним шляхом було прийдено до висновку, що найбільша точність отримується при першому кроці, а точність другого та третього – зменшується.
5. Експериментально продемонстровано використання LSTM нейронної мережі, що здатна адаптуватися до складних даних з великою кількістю варіативності.

References

1. Bzdok, D., Altman, N., Krzywinski, M. Statistics versus machine learning. 2018. pp. 233–234. [in English]. URL: https://doi.org/10.1038/nmeth.4642
2. *Brownlee J. Multi-Step LSTM Time Series Forecasting Models for Power Usage.* [in English]. URL: https://machinelearningmastery.com/how-to-develop-lstm-models-for-multi-step-time-series-forecasting-of-household-power-consumption/
3. Verma Y. Complete Guide To Bidirectional LSTM (With Python Codes). [in English]. URL: https://analyticsindiamag.com/complete-guide-to-bidirectional-lstm-with-python-codes/
4. Feng W., Tang J,, Xiao Liu T., Zhang S., Guan J. Proceedings of the 33rd AAAI Conference on Artificial Intelligence. 2019.Dataset. [in English]. URL: http://moocdata.cn/data/user-activity#User%20Activity
5. Dolphin R. LSTM Networks | A Detailed Explanation. [in English]. URL: https://towardsdatascience.com/lstm-networks-a-detailed-explanation-8fae6aefc7f9

УДК 004.056

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ДЕРЖАВНОГО СЕКТОРУ НА ОСНОВІ SIEM-СИСТЕМ

DOI 10 36994 / 2788- 5518- 2022-02-04-14

Кошара А.В. *Державний університет інтелектуальних технологій і зв'язку, Київ, Україна. artemkosharaa@gmail.com*

Бакало Б.В. *. Відкритий міжнародний університет розвитку людини «Україна»,Київ,Україна. konstantin.bogdanbakalo@.gmail.com*

Анотація: *У статті розглядається актуальність експлуатації SIEM-систем задля організації захисту інформаційно-телекомунікаційних систем та оперативного виявлення кібератаки, своєчасне реагування на таку атаку для якісного розслідування інциденту кібератаки направленої на державні установи та оборонні підприємства держави. Наведено статистичні дані незалежних комерційних організацій та державного Держспецзв'язку, на тему найбільш вразливих категорій підприємств та найбільш ризикових векторів загроз. В статті викладено , що потреба в описаних системах обумовлена експоненційним зростанням кількості кіберзагроз, їх ускладненням і появою цілеспрямованих атак з використанням різних векторів проникнення. Цінність SIEM-системи полягає в тому, що вона збирає інформацію з різних систем та мережевих пристроїв, зберігає їх в одному місці та видає в доступному для аналізу вигляді, також система зберігає дані про всі події в мережі для розслідування інцидентів співробітниками відділу інформаційної безпеки. Тільки завдяки аналізу накопичених даних в SIEM, дозволяє визначити, стався інцидент вперше або подібні атаки були і в минулому. Проведено дослідження сучасних інструментів інформаційної безпеки, що входять до складу SIEM-систем, в розрізі моніторингу та реагування на інциденти інформаційної безпеки. Проведено огляд засобів SIEM-системи, що допомагають виявляти загрози інформаційної безпеки та оперативно реагувати на них. А саме: способи виявлення внутрішніх загроз, встановлення факту крадіжки даних, виявлення зловживання привілейованим доступом, виявлення компрометації довіреного пристрою, опис роботи та можливостей інструменту UBA, що базується на технології штучного інтелекту. Проведено огляд програмних складових (компонентів) SIEM-систем, з описом основних фунцій зазначених компонентів. Наведено рекомендації, щодо глибшого дослідження певних аспектів роботи SIEM-систем та систем наступного покоління – SOAR.*

Ключові слова: *кібербезпека, SIEM, атака, виявлення, реагування, держустанова, оборонний сектор.*

INCREASING SECURITY OF THE PUBLIC SECTOR BASED ON SIEM-SYSTEMS

Artem Koshara . *State University of Intellectual Technologies and Communication, Kyiv, Ukraine.artemkosharaa@gmail.com*

Bogdan Baralo. *Open International University of Human Development "Ukraine",Kyiv, Ukraine. bogdanbakalo@.gmail.com*

Abstract: *The article examines the relevance of using SIEM systems to organize the protection of information and telecommunication systems and the prompt detection of a cyber attack, timely response to such an attack for the qualitative investigation of an incident of a cyber attack directed at state institutions and defense enterprises of the state. Statistical data of independent commercial organizations*

and the state State Intelligence Service are given on the topic of the most vulnerable categories of enterprises and the most risky threat vectors. The article states that the need for the described systems is due to the exponential growth of the number of cyber threats, their complexity and the appearance of targeted attacks using various penetration vectors. The value of a SIEM system is that it collects information from various systems and network devices, stores it in one place and issues it in an accessible form for analysis, and the system also stores data about all events in the network for the investigation of incidents by employees of the information security department. Only thanks to the analysis of the accumulated data in SIEM, it is possible to determine whether the incident happened for the first time or whether similar attacks have occurred in the past. A study of modern information security tools, which are part of SIEM systems, was conducted in terms of monitoring and responding to information security incidents. An overview of the tools of the SIEM system, which help to detect threats to information security and promptly respond to them, was conducted. Namely: methods of detecting internal threats, establishing the fact of data theft, detecting the abuse of privileged access, detecting the compromise of a trusted device, describing the operation and capabilities of the UBA tool based on artificial intelligence technology. An overview of software components (components) of SIEM systems was conducted, with a description of the main functions of the specified components. Recommendations are given for a deeper study of certain aspects of the work of SIEM systems and systems of the next generation - SOAR.

Key words: *cyber security, SIEM, attack, detection, response, government agency, defense sector.*

Вступ

Більшість інформаційно-комунікаційних систем України сьогодні піддаються впливу різноманітних загроз інформаційної безпеки. Всього лише за перші 4 місяці повномасштабного воєнного вторгнення росії за даними Держспецзв'язку було проведено 796 кібератак на цифрову інфраструктуру України. Переважна більшість атак прийшлася саме на державний сектор: уряд і місцеві органи влади – 179 атак та сектор безпеки і оборони – 104 [1]. Загалом, загрози можуть надходити як ззовні, так і зсередини організації та можуть мати руйнівні наслідки. Атаки можуть повністю вивести з ладу системи або призвести до витоку конфіденційної, таємної інформації, що може суттєво вплинути на обороноздатність держави.

Для захисту держустанови та її локальної мережі тепер недостатньо звичайної антивірусної програми та міжмережевого екрану. Починаючи з другого десятиліття XXI століття, спектр потенційних загроз значно розширився, а число пристроїв, підключених до однієї комп'ютерної мережі, може становити більше декількох тисяч, при цьому знаходитися на різних континентах. Першим кроком до посилення стану захищеності мереж стало виявлення підозрілої активності, адже якщо загрозу було виявлено вчасно, то її нейтралізація та подальший захист від неї буде значно легшим кроком для підприємства, аніж усунення наслідків успішної для зловмисника кібератаки.

Вказані вище об'єми атак на дежрустанови підіймають наступні важливі питання: оперативне виявлення кібератаки, своєчасне реагування на таку атаку та зручний централізований засіб для аналізу подій інформаційної безпеки з IT-систем для якісного розслідування інциденту. Для покриття вищевказаних задач існують SIEM-системи.

Виконання досліджень

Системи Security Information and Event Management (управління інформацією та подіями безпеки), або скорочено SIEM - центральний елемент центру управління кібербезпекою (SOC) та є важливою частиною розвиненої системи захисту підприємства або державної організації. SIEM-системи збирають дані про інциденти від різних систем захисту, таких як фаєрволи, IPS, антивіруси. Також є можливість збирати дані з кінцевих пристроїв за допомогою агентів SIEM-системи. Системи управління інформацією та подіями безпеки дозволяють виявляти підозрілі і потенційно небезпечні ситуації. Крім того, ці системи скорочують затрати на інформаційну безпеку та ризики загроз безпеки, зменшуючи час на їх виявлення.

SIEM - система управління інформацією і подіями безпеки (англ. security information and event management) являє собою централізовану платформу реєстрації подій інформаційної безпеки, що дозволяє групам кібербезпеки аналізувати дані про події в режимі реального часу для раннього виявлення цільових кібератак і витоків даних. SIEM використовується як інструмент для збору, зберігання, дослідження і складання звітів за даними журналу для виявлення загроз, реагування на інциденти та для проведення

криміналістичної експертизи.

Потреба в зазначених системах обумовлена експоненційним зростанням кількості кіберзагроз, їх ускладненням і появою цілеспрямованих APT-атак, в тому числі з використанням різних векторів проникнення. SIEM може бути реалізована апаратно, або постачатися як програмне забезпечення (віртуальна машина), може бути розміщена, як в мережі замовника, так і віддалено - в хмарі. Цінність SIEM-системи полягає в тому, що вона збирає інформацію з різних систем та мережевих пристроїв, зберігаючи їх в одному місці та видає в доступному для аналізу вигляді, також система зберігає дані про всі події в мережі (успішна або неуспішна спроба введення паролю від облікового запису, активність вірусів, аномальний трафік, спроба підключення до кінцевого обладнання з використанням протоколів віддаленого доступу, тощо) для розслідування інцидентів співробітниками відділу інформаційної безпеки. Тільки SIEM здатна ефективно зафіксувати розвинену сталу загрозу (APT), при якій шкідливий код може бути присутнім в системах багато місяців до самого моменту активації. Завдяки аналізу накопичених даних SIEM дозволяє визначити, стався інцидент вперше або подібні атаки були і в минулому.

Щоб зрозуміти, наскільки важливу роль в забезпеченні інформаційної безпеки грають SIEM-системи, необхідно звернути увагу на масштаб інцидентів безпеки і задіяних в ньому даних. Велике підприємство здатне генерувати більше 25000 подій в секунду (EPS) і вимагати більше 50 ТБ для збереження даних. Здатність SIEM фільтрувати всі дані і визначати пріоритети найбільш критичних проблем інформаційної безпеки робить безпеку більш керованою. Ефективна SIEM-система виправдає витрати на неї за рахунок економії часу персоналу, навіть якщо сама система вимагає управління та налаштування. В процесі свого функціонування, кожен мережевий пристрій, додаток та кожна операційна система, записують усі події, що відбуваються з ними в журнали реєстру. Завдяки даним, що записані в журналах подій (логах), SIEM може проаналізувати поведінку системи чи користувача, провести оцінку ризиків, враховуючи критичність активів та порушенню на них директив кореляції та надати оцінку захищеності інфраструктури. Наприклад, можна визначити, які саме операції відбувалися в системі на момент порушення директиви кореляції.

В звіті Verizon «Data Breach Investigation Report» зазначено, що 60% основних порушень безпеки були пов'язані з інсайдерськими (внутрішніми) загрозами, інсайдерські загрози залишаються непоміченими протягом місяців (в 42% випадків) або років (38% випадків) [2]. Виявлення інсайдерських загроз є складним завданням - поведінка не викликає підозри в більшості інструментів безпеки, тому що зловмисник є легітимним користувачем. SIEM може виявити індикатори внутрішніх загроз за допомогою поведінкового аналізу, допомагаючи службам інформаційної безпеки виявляти і запобігати атакам завдяки SIEM-системам наступного покоління, які використовують технологію «user behavior analytics» (UBA). Технологія UBA використовує машинне навчання і поведінковий аналіз для визначення базових показників IT-користувачів і систем та інтелектуального виявлення аномалій, що виходять за рамки правил і статистичних кореляцій, які використовуються в SIEM.

Звіт RiskBased Security про порушення конфіденційності даних показав, що виявлено 3932 публічно зареєстрованих випадків витоку даних, в результаті яких було скомпрометовано більш 37 мільярдів записів. У порівнянні з 2019 роком кількість публічно заявлених порушень скоротилася на 48%. Однак загальна кількість скомпрометованих записів збільшилася на 141% і на сьогоднішній день є найбільшою кількістю записів, виявлених за один рік з моменту створення звітності RBS (RiskBased Security) в 2005 році. Було зафіксовано 676 порушень, в яких елементом атаки використовувалися програми-вимагачі, що на 100% більше, ніж в 2019 році [3]. Зростання числа програм-вимагачів в поєднанні з практикою витоку даних, вкрадених під час атаки являли собою головні теми 2022 року для обговорення центрів кіберзахисту, як підприємств різного масштабу, так і центрів кіберзахисту держав по всьому світу.

Сектор охорони здоров'я виявився найбільш постраждалим, на нього довелося 12,3% зареєстрованих порушень. Медичні служби, підприємства роздрібної торгівлі та державні установи зазнали найбільших збитків. Деякі з цих секторів більш привабливі для

кіберзлочинців, тому що вони містять фінансові та медичні дані. Але незважаючи на попередній тезис, всі підприємства що використовують комп’ютерні мережі, є потенційними мішенями для кібератак або корпоративного шпигунства.

International Data Corporation прогнозує, що з урахуванням того, що масштаби кіберзагрози будуть зростати, до 2022 року світові витрати на рішення для кібербезпеки сягатиме 133,7 млрд доларів [4]. Уряди по всьому світу відреагували на зростаючу кількість кіберзагроз, надавши рекомендації з надання допомоги організаціям, що впроваджують ефективні методи кібербезпеки. Наприклад, національний інститут стандартів і технологій (NIST) США створив «Cybersecurity Framework» для боротьби з поширенням шкідливого коду і допомоги в ранньому виявленні. Система виконує безперервний моніторинг всіх електронних ресурсів в режимі реального часу.

SIEM-система здатна «полювати на загрози». Це практика активного пошуку кіберзагроз в організації або мережі. Полювання на загрози може проводитися відразу після інциденту безпеки, але також і в превентивному режимі для виявлення нових або невідомих атак або порушень. Для пошуку загроз необхідний широкий доступ до даних безпеки з усієї організації, який може бути наданий SIEM.

Способи, якими SIEM-система допомогає в процесі пошуку загроз включають в себе: повіщення від систем безпеки, які надають контекст і дані, що допомагають розслідувати потенційний інцидент, виявлення аномалій в IT-системах за допомогою кореляції та поведінкової аналітики, пошук серед історичних даних шаблонів атак або сигнатур, аналогічних відомим атакам, поєднання аналітики загроз з даними безпеки для інтелектуального виявлення атак в IT-системах, створення попереджень, заснованих на відомих ризиках, що допомагають аналітикам інформаційної безпеки сформулювати гіпотезу і перевірити її, досліджуючи дані безпеки в SIEM, перевірка, чи було зафіксовано подібний інцидент раніше - пошук в даних інформаційної безпеки шаблонів, схожих на поточний або попередній інцидент безпеки.

Виявлення зловживання привілейованим доступом SIEM-системою: моніторинг і звітність про підозрілий доступ до конфіденційних даних, моніторинг активності зовнішніх постачальників і партнерів, що мають доступ до інформаційних систем організації, з метою виявлення аномальної поведінки або підвищення привілеїв, попередження про будь-якої активності припинених облікових записів користувачів або несподіваної активності в облікових записах, які зазвичай неактивні, попередження про аномальну активність, що може бути катастрофічною людською помилкою, наприклад, при видаленні великих обсягів даних, створення звітів про користувачів, які звертаються до систем або даних, які виходять за рамки їх звичайного профілю використання.

Виявлення компрометації довірених осіб SIEM-системою: виявлення аномальної активності, попередження про це і надання даних, необхідних для встановлення факту того, чи було скомпрометовано обліковий запис привілейованого користувача, створення базових показників активності серверів, виявлення відхилень від базових показників і оповіщення співробітників центру кібербезпеки, моніторинг трафіку, виявлення аномальних сплесків, використання незахищених протоколів передачі даних, антивірусний моніторинг - шкідливе програмне забезпечення є частою точкою входу для компрометації хоста. SIEM моніторить антивірусні системи захисту, розгорнуті на кінцевих пристроях та повідомляють про такі події, як відключення антивірусного захисту, видалення антивірусу.

Встановлення факту крадіжки даних SIEM-системою: виявлення мережевого трафіку до центрів управління та контролю, виявлення заражених систем, що передають дані неавторизованих сторонам, моніторинг мережевого трафіку по протоколах, які полегшують передачу великих обсягів даних, і попередження, коли передаються незвичайні обсяги або типи файлів, або коли мета невідома або є шкідливою, моніторинг використання веб-додатків організації або внутрішнього використання зовнішніх веб-додатків, що може включати завантаження або доступ браузера до конфіденційних даних, виявлення електронних листів, переадресованих або відправлених іншим особам, крім зазначеного одержувача, крадіжка даних зазвичай пов'язана зі спробами зловмисників підвищити привілеї або отримати доступ до інших IT-систем. SIEM-система може виявляти вказані вище дії шляхом зіставлення даних з декількох IT-систем, відстеження даних від

мобільних пристроїв співробітників і виявляти аномалії, які можуть вказувати на витік інформації через мобільний пристрій.

Виявлення внутрішніх загроз є складним завданням - поведінка не викликає підозри в більшості інструментів безпеки, тому що зловмисник є легітимним користувачем. SIEM може виявити індикатори внутрішніх загроз за допомогою поведінкового аналізу, допомагаючи службам інформаційної безпеки виявляти і запобігати таким загрозам завдяки технології «user behavior analytics» (UBA). Технологія UBA використовує машинне навчання і поведінковий аналіз для визначення базових показників IT-користувачів і систем та інтелектуального виявлення аномалій, що виходять за рамки правил і статистичних кореляцій.

Способи, якими SIEM-системи допомогають зупинити інсайдерські загрози: поведінковий аналіз для виявлення аномальної поведінки користувачів, вказуючих на компрометацію. Наприклад, вхід в систему в незвичайний час доби з незвичайною частотою або доступ до незвичайних даних або систем, SIEM виявляє, що користувачі змінюють або підвищують привілеї для критично важливих систем, SIEM співвідносять мережевий трафік з даними про загрози, щоб виявляти шкідливі програми, які взаємодіють із зовнішніми зловмисниками. Це ознака зламаного облікового запису користувача, поведінковий аналіз для аналізу подій інформаційної безпеки, таких як вставка флеш-накопичувачів USB, використання особистих поштових сервісів, несанкціонованого хмарного сховища або надмірного друку документів, виявлення і зупинення шифрування великих обсягів даних, адже це може вказувати на атаку програми-шифрувальника, інсайдери, які проводять атаку, можуть спробувати вимкнути облікові записи, машини і IP-адреси на шляху до мети. SIEM можуть виявити це поведінку, тому що мають широкий огляд IT-систем.

Типове рішення SIEM-системи включає в себе кілька функціональних компонентів, що зображені на рисунку 1: агент (сервіс, демон), що встановлюється на систему, яку необхідно моніторити, локально збирає журнали подій і за наявності заздалегідь налаштованого мережевого маршруту передає їх до SIEM-систему), лог-колектори, що призначені для попередньої акумуляції подій від безлічі джерел, кореляція, що опрацьовує інформацію від колекторів за встановленими правилами і алгоритмами кореляції, бази даних і сховища для зберігання, як опрацьованих, так і неопрацьованих журналів подій.

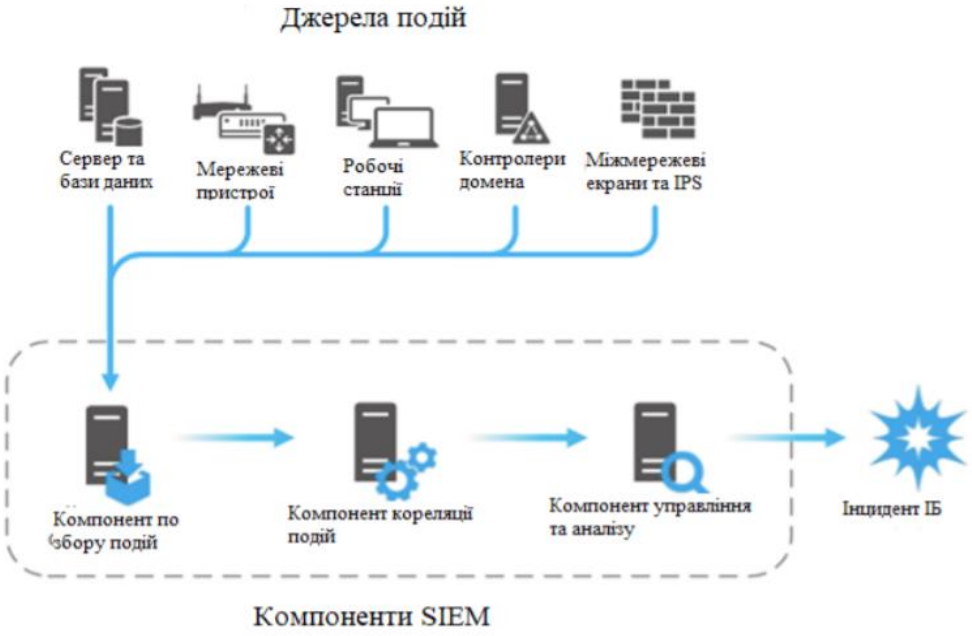


Рис. 1. Основні компоненти SIEM-системи

Висновки

SIEM-система є найнеобхіднішим сучасним інструментом кібербезпеки для державних установ та бізнесу, як в мирний, так особливо і в воєнний час. Адже в обставинах безперервних, як ракетних, так і кібератак, оперативне реагування є ключовою складовою убезпечення життя, як людського, так і життя оборонного сектору держави, а отже і держави вцілому. Наявність великої кількості описаних інструментів у складі SIEM-системи, дозволяє експлуатувати її у відповідності до особливостей діяльності підприємства та задач інформаційної безпеки, що перед ним стоять.

Перспектива подальших досліджень вбачається в ґрунтовнішому вивченні використання інструменту UBA, що базується на технології штучного інтелекту та у висвітленні актуальності експлуатації системи SOAR, як наступного кроку у розвитку автоматизованого реагування на інциденти кібербезпеки.

Література

1. Держспецзв'язку. Статистика кібератак за чотири місяці війни. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
2. Verizon. 2022 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/
3. RiskBased Security Report. URL: https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report
4. International Data Corporation Report. URL: https://www.idc.com/getdoc.jspcontainerId=prUS46773220
5. Microsoft. What Is SIEM. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem
6. What Is SIEM, Why Is It Important and How Does It Work? URL: https://www.exabeam.com/explainers/siem/what-is-siem/
7. SIEM Architecture: Technology, Process and Data. URL: https://www.exabeam.com/explainers/siem/siem-architecture/
8. Everything You Need to Know about SIEM Architecture. URL: https://wisdomplexus.com/blogs/siem-architecture/

References

1. Derzhspeczv'yazku. Statistika kiberatak za chotiri misyaci vijni. [Statistics of cyberattacks for four months of the war]. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
2. Verizon. 2022 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/
3. RiskBased Security Report. URL: https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report
4. International Data Corporation Report. URL: https://www.idc.com/getdoc.jspcontainerId=prUS46773220
5. Microsoft. What Is SIEM. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem
6. What Is SIEM, Why Is It Important and How Does It Work? URL: https://www.exabeam.com/explainers/siem/what-is-siem/
7. SIEM Architecture: Technology, Process and Data. URL: https://www.exabeam.com/explainers/siem/siem-architecture/
8. Everything You Need to Know about SIEM Architecture. URL: https://wisdomplexus.com/blogs/siem-architecture/

УДК 004.4

КЕРУВАННЯ КЛІЄНТСЬКИМИ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ З ДИНАМІЧНИМ ЖИТТЄВИМ ЦИКЛОМ У КОРПОРАТИВНІЙ МЕРЕЖІ

DOI 10 36994 / 2788- 5518- 2022-02-04-15

Смаглюк В.О. *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. amxleclerk@gmail.com*
Алєксєєв М.О.*, к.т.н. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна. n.alexeyev@gmail.com*

Анотація: *Робота присвячена актуальному питанню ефективного використання обчислювальних ресурсів в системах з динамічною розподіленою архітектурою, які застосовують обчислювальні пристрої персональні або загального користування для потреб розподілених обчислень, а саме задачі ефективного керування життєвим циклом робочих вузлів кластерів контейнеризованих застосунків. На відміну від відомих існуючих рішень, системи, які розглядаються у роботі, мають відносно короткостроковий і недетермінований час життя своїх обчислювальних агентів і тому повинні мати спеціалізований функціонал для автоматичного під'єднання та відключення обчислювальних агентів від кластеру, оскільки сам процес приєднання нового робочого вузла до такої системи займає певний час, і потребує певної кваліфікації і рівня авторизації. Якщо ж ввести у систему додатковий адміністративний вузол, що буде вирішувати питання налаштування нових клієнтів, ми в рази збільшуємо оперативне навантаження на такий управляючий об'єкт. Необхідно надати прозорий інтерфейс (процес на декілька дій) для користувача і при цьому автоматизувати будь-які повторювані дії зі сторони оператора Kubernetes кластеру. Запропонований у роботі підхід базується на організації процесу керування робочими вузлами на зразок Server Discovery у середовищі Kubernetes кластеру. Перевагою запропонованого підходу є гнучкий та простий інтерфейс керування робочими вузлами з недетермінованим життєвим циклом у корпоративній мережі на основі підготовлених програм, що виконують операції з перевірки операційного середовища користувача, інсталяції необхідного програмного забезпечення для приєднання до обчислювальної системи або ж деінсталяції компонентів та відключення агента за вимогою користувача. У роботі розглянуто експериментальне середовище, проведено дослідження роботи системи у можливих сценаріях поведінки користувача та обґрунтована ефективність підходу.*

Ключові слова: *розподілена обчислювальна система, Kubernetes кластер, керування життєвим циклом обчислювальних вузлів.*

MANAGEMENT OF CLIENT COMPUTING RESOURCES WITH A DYNAMIC LIFE CYCLE IN A CORPORATE KUBERNETES CLUSTER NETWORK

Volodymyr Smahliuk. *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine. amxleclerk@gmail.com*
Nikolay Alieksieiev*, Ph,D, Ass. Prof. National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine. n.alexeyev@gmail.com*

Abstract: *The work is dedicated to the topical issue of effective use of computing resources in systems with a dynamic distributed architecture, which use personal or public computing devices for the needs of distributed computing, in particular the paper is devoted to the task of effective management of the life cycle of working nodes of clusters of containerized applications. Unlike the known existing solutions, the systems considered in the work have a relatively short-term and non-deterministic lifetime of their computing agents and therefore must have specialized functionality for automatically joining and*

detaching computing agents from the cluster as far as the process of joining a new working node to such a system takes a certain amount of time and requires a certain qualification and level of authorization. If we inject an additional administrative node into the system, which will solve the issue of setting up new clients, we will increase the operational load on such a control object. It is necessary to provide a transparent interface (few clicks process) for the user and at the same time automate any repetitive actions on the part of the Kubernetes cluster operator. The approach proposed in the work is based on the organization of the process of managing working nodes such as Server Discovery in the Kubernetes cluster environment. The advantage of the proposed approach is a flexible and simple interface for managing working nodes with a non-deterministic life cycle in the corporate network based on prepared programs that perform operations of checking the user's operating environment, installing the necessary software to connect to the computer system, or uninstalling components and disabling the agent on user demand. The paper describes the experimental environment, conducts a study of the system's operation in possible user behavior scenarios and proves the effectiveness of the approach.

Key words: *distributed computing system, Kubernetes cluster, management of nodes life cycle.*

Вступ

Для підвищення ефективності використання незайнятих ресурсів обчислювальних вузлів та зниження загального рівня їх простоювання і водночас, для вирішення нагальних завдань з розміщення та виконання програмних компонентів корпоративних інформаційно-обчислювальних систем раніше у роботі було вирішено створювати кластери із залученням персональних пристроїв користувачів корпоративної мережі, а також парку комп'ютерної техніки та загальнодоступних обчислювальних пристроїв у корпоративній мережі. Також було прийняте рішення щодо використання контейнеризації прикладних програм та програмної технології Kubernetes для оркестрації робочих навантажень на їх основі, оскільки цей підхід дозволяє використовувати апаратні і програмні обчислювальні ресурси різні за походженням і характеристиками, а також дає змогу підключати і від'єднувати їх у процесі експлуатації [1]. Вузол Kubernetes (node, "нода") або робочий вузол у даному контексті це фізична або віртуальна машина, яка бере участь у кластері Kubernetes, і яку можна використовувати для запуску робочих навантажень (pod, "под") у вигляді контейнеризованих програм. Проте, процес долучення та від'єднання робочих вузлів потребує виконання певних операцій у ручному режимі. Користувач, що хоче надати обчислювальні потужності свого пристрою для виконання прикладних програм у корпоративному кластері, повинен самостійно підготувати систему, а саме:

- перевірити сумісність клієнтської системи з цільовою кластерною мережею;
- встановити необхідне клієнтське програмне забезпечення за вимогами його операційної системи;
- ініціалізувати запит на приєднання до Kubernetes кластеру.

За необхідності користувач повинен мати можливість від'єднатися від обчислювальної системи і безпечно очистити будь-які артефакти, що могли залишитися після налаштування зв'язку з цільовою системою, включаючи клієнтське програмне забезпечення. Також, необхідно врахувати сценарії, за яких клієнт більше не доступний для розміщення на ньому прикладних програм (чи то через проблеми з мережею, чи через санкціоновані дії клієнта спрямовані на розірвання зв'язку з системою) і реагувати у відповідності з конкретними причинами.

Враховуючи це, можна виділити три основні можливі стани клієнта:

1) готовність – клієнт готовий ініціалізувати запит на приєднання;
2) активний режим – клієнт є частиною розподіленої системи та надає свої незайняті ресурси для прикладних обчислень;
3) неактивний режим – клієнт більше не надає свої ресурси або зв'язок з ним втрачено, але він досі числиться у списку робочих вузлів.

Для вирішення цих проблем можна ввести додатковий керуючий вузол (адміністратор), який буде налаштовувати цільові системи.

При невеликій кількості потенційних клієнтів адміністратор Kubernetes кластеру може сам проконтролювати переходи між станами та виконувати конфігураційні задачі, а саме: ініціалізацію програмного забезпечення, аналіз відповідності наданого пристрою до вимог цільової системи або видалення його. Проте, зі збільшенням кількості робочих пристроїв N буде зростати операційне навантаження P на адміністративний вузол за певним експоненціальним законом $P = exp(N)$, що призводить до складностей коректного налаштування та підтримки таких систем.

Якщо додатково врахувати, що система є динамічною, тоді час життя робочих пристроїв не обов’язково буде збільшуватися за лінійним законом, що є справедливим для системи зі статичними пристроями, постійно під’єднаними до системи. Навіть навпаки: збільшення частоти переходу між можливими станами призводить до додаткових операційних навантажень, оскільки треба відслідковувати та вести звітність про кожен з клієнтів: у якому стані вони знаходяться, а також які дії потрібно виконати, щоб безпечно перевести пристрій з одного в інший стан.
Досвідчені користувачі можуть самі налаштовувати свою систему за потреби, але у загальному випадку, клієнт повинен мати зручний інтерфейс для під’єднання до цільової системи без додаткових операційних навантажень зі свого боку.

Виконання досліджень

Враховуючи усе вище згадане, необхідно вирішити дві основні проблеми для зменшення кількості адміністративної роботи або, за можливості, уникнути будь-якої додаткової взаємодії з ним.

Першою з проблем є ведення актуальної таблиці станів робочих пристроїв. Загалом такий механізм називається Service Discovery, де у ролі сервіса виступає робочий вузол (“нода”). Service Discovery створений для того, щоб з мінімальними витратами можна підключити новий сервіс до нашого оточення.
У нашому випадку це питання вирішується за допомогою інтегрування певної бази даних. У середовищі Kubernetes кластеру цю функцію виконує програмне забезпечення etcd.
База даних etcd є послідовним розподіленим сховищем у форматі ключ-значення. Це ПЗ використовується як окрема служба координації в розподілених системах. Воно призначене для зберігання невеликих обсягів даних, які можуть повністю поміститися в оперативній пам’яті [2]. Цей компонент зберігає всю інформацію про робочі навантаження, які представлені у системі, враховуючи облік нод. За допомогою інтерфейсу Kubernetes API ця інформація періодично оновлюється, щоб відповідати реальному станові системи.
Таким чином, etcd веде інформацію про два стани нод: активний (*Ready*) та неактивний (*NotReady*) (рис. 1).

```
NAME                 STATUS    ROLES   AGE     VERSION
master.example.com   Ready     master  5h      v1.23
node1.example.com    NotReady  compute 5h      v1.23
node2.example.com    Ready     compute 5h      v1.23
```

Рис. 1. Приклад відображення станів робочих вузлів (“нод”) Kubernetes кластеру

Якщо у etcd немає інформації про певну з нод, тоді вважається, що вона перебуває у стані готовності до ініціалізації. Навіть у випадку, коли пристрій користувача було вилучено із кластеру, але програмні компоненти досі встановлено на його машині, він знову має пройти етап ініціалізації запиту на приєднання до розподілювальної системи.
Друга проблема полягає в тому, як зменшити операційне навантаження на адміністративний вузол під час підготовки клієнтської системи до приєднання до кластерної мережі. Для вирішення цього питання пропонується використовувати автоматизований пакет (скрипт), який перевірить систему на відповідність вимог цільової кластерної мережі, інсталює необхідні програмні пакети та приєднає клієнтський пристрій до Kubernetes.
Ідея полягає в тому, щоб надати доступне (в рамках корпоративної мережі) посилання на єдиний виконувальний файл, який в залежності від сценарію буде мати різний алгоритм дій. Бажаний сценарій можна буде обрати додаючи різні опції під час запуску скрипту.
Розглянемо більш детально кожен із сценаріїв, які реалізує програмний код, та порядок дій для кожного з них.

1. Реєстрація робочих вузлів:
    a. Ініціалізація запиту на приєднання (запит на адресу http://cluster.local/script)
    b. Отримання скрипту на встановлення компонентів
    c. Запуск скрипту з флагом *--init*

i. Перевірка системи (os-release) та вимог цільової системи до ресурсів пристрою;
ii. Перевірка встановлених пакетів;
iii. Встановлення пакеті, якщо таких не було знайдено в системі.

d. Ініціалізація з’єднання до кластеру
e. З’єднання встановлено

Блок-схему наведеного алгоритму зображено на рис. 2. По завершенню сценарію клієнтський пристрій переходить зі стану “готовності до ініціалізації” в стан “активний режим”.

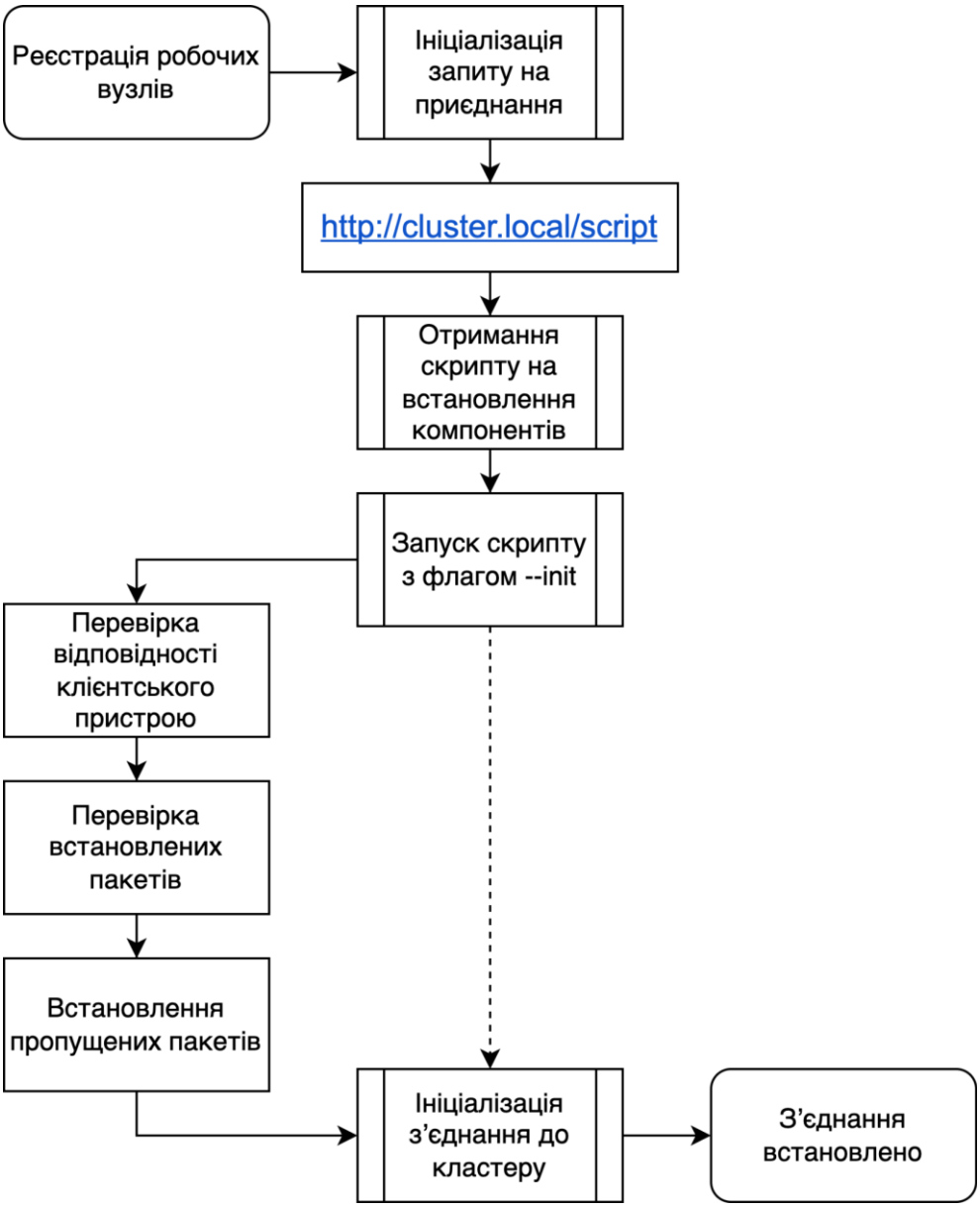


Рис. 2. Блок-схема процесу реєстрації робочих вузлів

2.Вилучення робочих вузлів:

f. Ініціалізація запиту на вилучення (запит на адресу http://cluster.local/script)
g. Отримання скрипту на видалення компонентів
h. Запуск скрипту з флагом *--reset*
i. Перевірка системи (os-release)
ii. Перевірка встановлених пакетів
iii. Видалення пакетів
i. Команда на роз’єднання від кластеру

j. Сервер від’єднано від кластеру

Блок-схему наведеного алгоритму зображено на рисунку 3. По завершенню сценарію клієнтський пристрій переходить зі стану “активний режим” в стан “готовність до ініціалізації”, не зважаючи на те, що приєднання не планується.

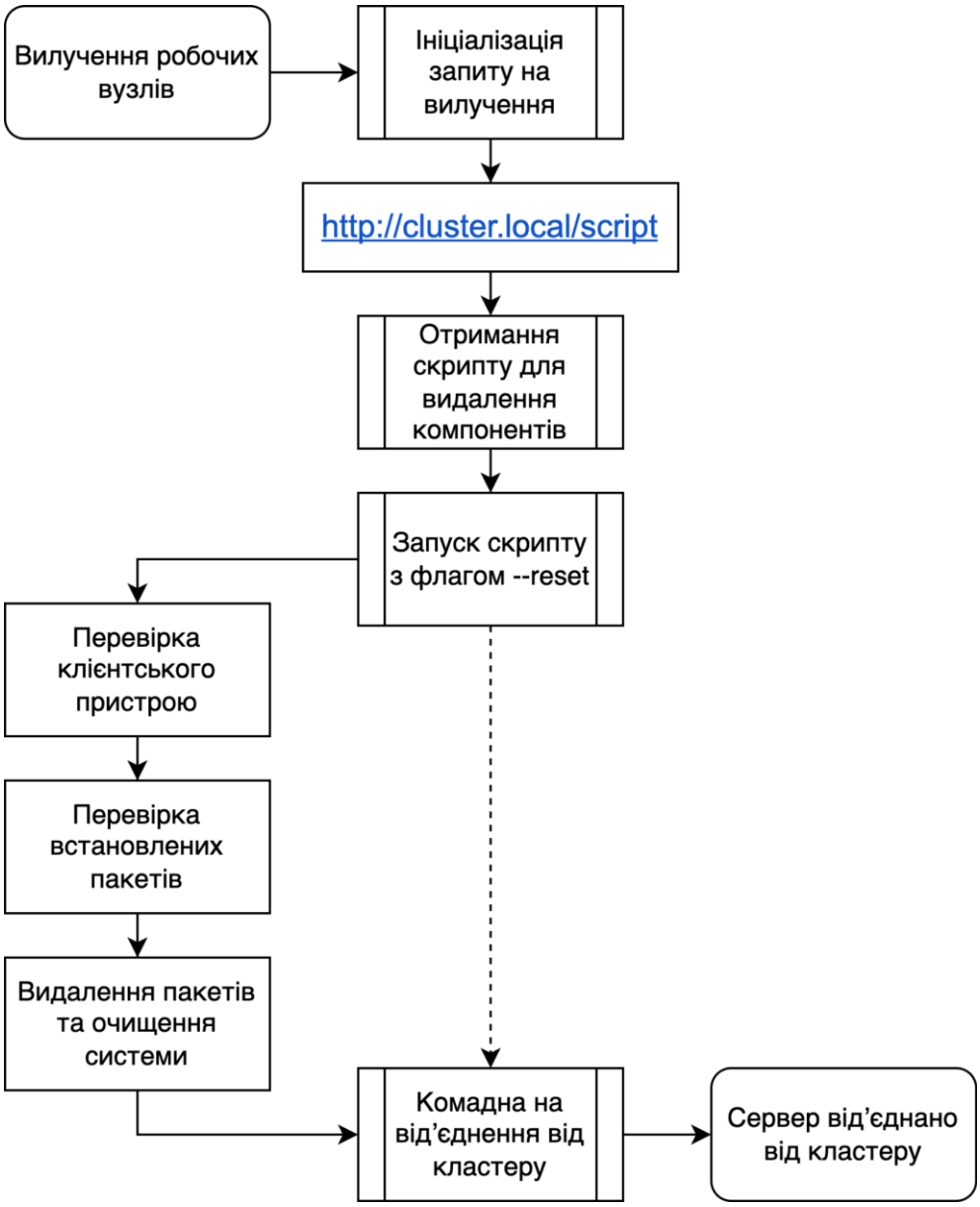


Рис. 3. Блок-схема процесу від’єднання робочих вузлів

Наведені два сценарії контролюються спеціальним програмним кодом, що отримує клієнт із відповідної адреси. Проте, може бути ситуація, коли було втрачено зв’язок із робочим вузлом. У такому випадку, робочий вузол переводиться у стан “неактивний режим”. Коли вузол вимикається або виходить з ладу, він переходить у стан NotReady, тобто його не можна використовувати для запуску подів (розподілених прикладних програм). Після цього всі поди, запущені на вузлі, стають недоступними [3]. Проте, варто наголосити, що робочі навантаження досі закріплено за проблемним вузлом.

Поширеними причинами *Node NotReady* помилки Kubernetes є

- брак ресурсів на вузлі, проблему з kubelet (агентом, який дозволяє Kubernetes сервісам отримувати доступ до вузла і та контролювати його роботу);
- помилку, пов’язану з kube-proxy (мережевий агент на вузлі);
- проблему з мережею в цілому.

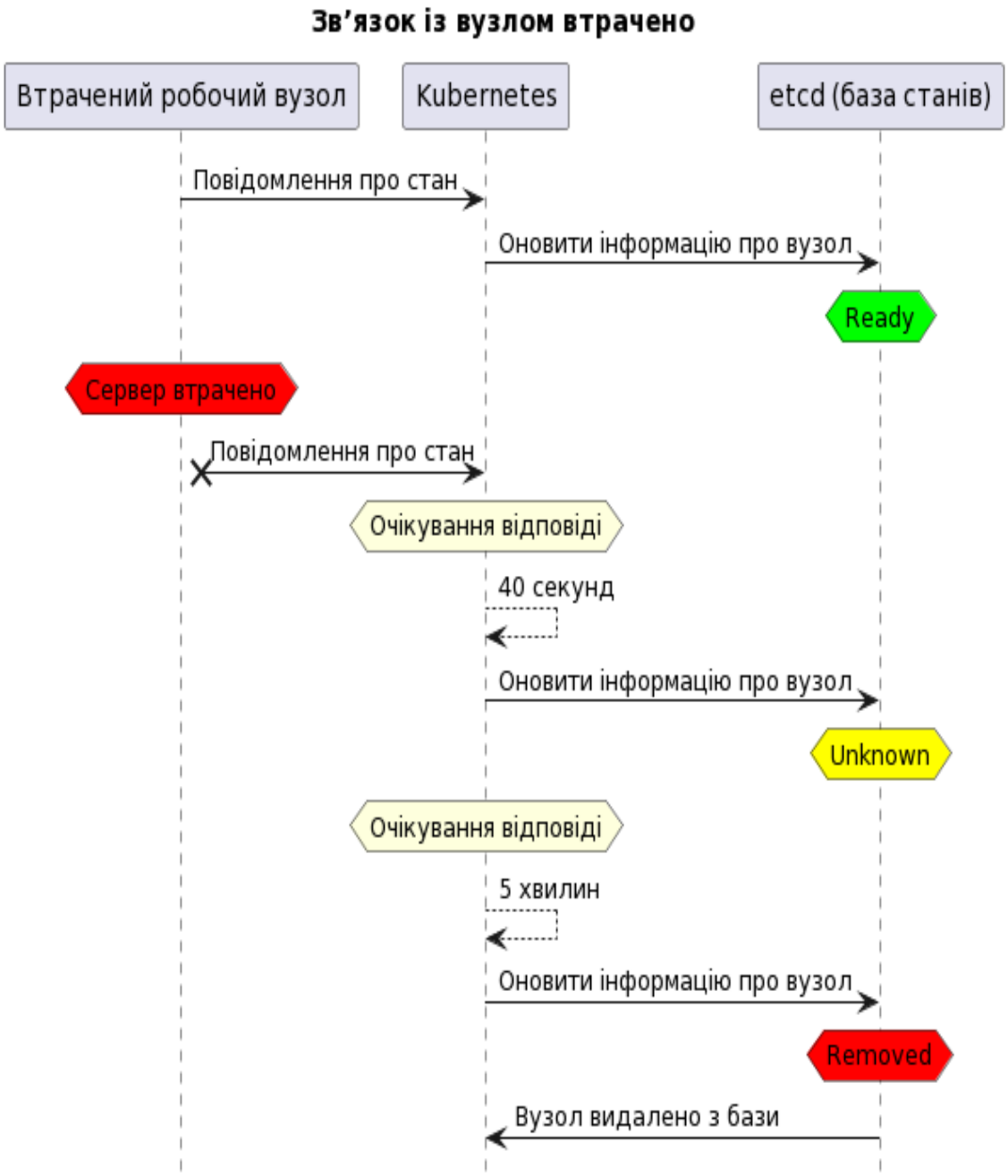


Рис. 4. Діаграма послідовностей у випадку втрати зв’язку з робочим вузлом

Якщо Kubernetes не може зв’язатися з вузлом, він чекає за замовчуванням 40 секунд, а потім встановлює статус вузла на *Unknown* або невідомий. Якщо вузол залишається недоступним відбувається ініціювання виселення за допомогою API для всіх подів на недоступному вузлі. За замовчуванням контролер вузла чекає 5 хвилин між позначенням вузла як невідомого та поданням першого запиту на вилучення [4]. Якщо недоступний вузол не повернувся до мережі, його буде видалено із внутрішньої бази (див. рис. 4), що у термінах даної статті означає переведення у стан “готовності до ініціалізації”.

У випадку повторного приєднання втраченого робочого вузла після того, як його було видалено з Kubernetes кластеру, клієнт повинен повністю пройти процес ініціалізації описаний вище (див. рис. 2).

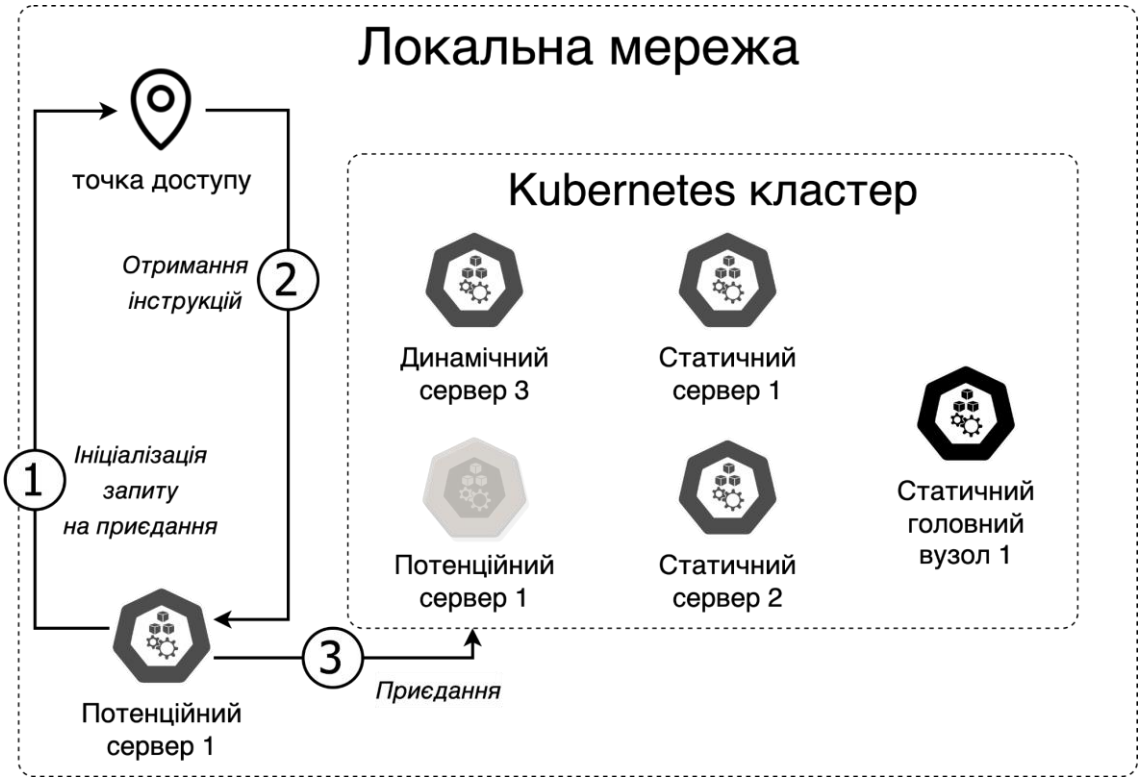


Рис. 5. Схема експериментального макету

Експериментальний макет (див. рис. 5) містить один головний вузол, два робочі статичні вузли, один динамічний вузол (у стані “активний режим”), потенційний динамічний вузол (у стані “готовність до ініціалізації”) та точку доступу (в рамках корпоративної мережі) з виконувальним програмним кодом. Повна інформація про зареєстровані робочі вузли наведена на рисунку 6.

```
NAME                STATUS   ROLES    AGE   VERSION
master.static.com   Ready    master   12h   v1.23
node1.static.com    Ready    compute  12h   v1.23
node2.static.com    Ready    compute  12h   v1.23
node3.dynamic.com   Ready    compute  10h   v1.23
```

Рис. 6. Список робочих вузлів Kubernetes кластеру

Для приєднання нового вузла до кластеру достатньо завантажити код та запустити його з опцією *--init* (рис. 7).

Відповідно, після успішного завершення скрипта ми побачимо новий робочий вузол node4.dynamic.com (рис. 8), запис про який збережено у ectd.

Процес вилучення відбувається під час запуску програмного скрипта з опцією *--reset* (рис. 9). Для чистоти експерименту, було запущено запит на видалення для node3.dynamic.com.

Kubernetes кластер реагує на архітектурні зміни. Робочий вузол більше не є частиною обчислювальної мережі, як можна побачити на рис. 10.

```
bash-3.2$ sh ./script.sh --init
# System information
Target OS: Ubuntu 22.04.1 LTS
System resources check: passed


# Kubernetes information
Target Kubernetes version: 1.23.13
Installation kubernetes packages: kubeadm, kubelet, kubectl
Successfully installed kubernetes packages.


# Docker information
Target Docker version: 20.10.8
Installation docker packages: docker-ce, docker-ce-cli, containerd.io
Successfully installed docker packages.


# Joining the cluster
Successfully joined the cluster.
```

Рис. 7. Процес ініціалізації нового динамічного вузла до Kubernetes кластеру

```
NAME                STATUS    ROLES   AGE     VERSION
master.static.com   Ready     master  13h     v1.23
node1.static.com    Ready     compute 13h     v1.23
node2.static.com    Ready     compute 13h     v1.23
node3.dynamic.com   Ready     compute 11h     v1.23
node4.dynamic.com   Ready     compute 6m      v1.23
```

Рис. 8. Список робочих вузлів Kubernetes кластеру після додавання нового вузла

```
bash-3.2$ sh ./script.sh --reset

# System information
Target OS: Ubuntu 22.04.1 LTS

# Kubernetes information
Target Kubernetes version: 1.23.13
Removing kubernetes packages: kubeadm, kubelet, kubectl
Successfully removed kubernetes packages.

# Docker information
Target Docker version: 20.10.8
Removing docker packages: docker-ce, docker-ce-cli, containerd.io
Successfully removed docker packages.

# Reset the cluster
Successfully rested the cluster.
```

Рис. 9. Процес вилучення динамічного вузла до Kubernetes кластеру

```
NAME                STATUS    ROLES   AGE     VERSION
master.static.com   Ready     master  13h     v1.23
node1.static.com    Ready     compute 13h     v1.23
node2.static.com    Ready     compute 13h     v1.23
node4.dynamic.com   Ready     compute 20m     v1.23
```

Рис. 10. Список робочих вузлів Kubernetes кластеру після видалення динамічного вузла

На рис.11 зображено поточну кластерну мережу відносно доступних робочих вузлів. Видаленого серверу 3 більше не існує у мережі.

Рис. 11. Кінцевий стан системи

Програмний код запропонованого рішення буде розміщено у публічному доступі за посиланням: https://github.com/VolodymyrSmahliuk/k8s-dynamic-node-operator

Висновки

1. Завдяки програмному коду вдалося мінімізувати оперативне навантаження на адміністратора Kubernetes кластеру, стосовно управління життєвим циклом робочих вузлів та їх підготовкою до приєднання у систему.
2. Запропонований метод дозволяє автоматизувати процес реєстрації та вилучення робочих вузлів до Kubernetes кластеру, що дає можливість побудувати динамічну обчислювальну систему з робочими вузлами з короткостроковим і недетермінованим часом життя своїх обчислювальних агентів.

Література

1. Смаглюк, В. О., Алєксєєв, М. О. Використання обчислювальних потужностей мобільних пристроїв та пристроїв інтернету речей у корпоративній мережі. *Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій»*, 2021. С. 238-240.
2. Docker Documentation: Docker architecture. 2021. URL: https://docs.docker.com/get-started/overview/#docker-architecture.
3. Etcd Documentation: “What is etcd?”, 2022. URL: https://etcd.io/docs/v3.5/faq/#what-is-etcd.
4. Luksa, Marko. *Kubernetes in action*. Simon and Schuster, 2017.
5. Kubernetes Documentation: Kubernetes Nodes: Conditions, 2022. URL: https://kubernetes.io/docs/concepts/architecture/nodes/#condition.

References

1. Smahlyuk, V. O., Alyeksyeyev, M. O. Vykorystannya obchyslyuval'nykh potuzhnostey mobil'nykh prystroyiv ta prystroyiv internetu rechey u korporatyvniy merezhi. [Quotation of the number of pressures of mobile devices and Internet speeches at corporate]. *Zbirnyk materialiv Mizhnarodnoyi naukovo-tekhnichnoyi*
2. *konferentsiyi «Perspektyvy telekomunikatsiy*», 2021.S, 238-240.
Docker Documentation: Docker architecture. 2021. URL: https://docs.docker.com/get-\
started/overview/#docker-architecture.
4. Etcd Documentation: “What is etcd?”, 2022. URL: https://etcd.io/docs/v3.5/faq/#what-is-etcd.
5. Luksa, Marko. *Kubernetes in action*. Simon and Schuster, 2017.
Kubernetes Documentation: Kubernetes Nodes: Conditions, 2022. URL:
https://kubernetes.io/docs/concepts/architecture/nodes/#condition

УДК 004.056.52

ДОСЛІДЖЕННЯ АЛГОРИТМІВ МОРФОЛОГІЧНОГО АНАЛІЗУ У DLP-СИСТЕМАХ ДЛЯ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

DOI 10 36994 / 2788- 5518- 2022-02-04-16

Близнюк А.В. *Державний університет інтелектуальних технологій і зв'язку, Київ,Україна. blizniykartem@gmail.com*

Анотація: *У статті досліджується використання морфологічного методу аналізу текстової інформації в системах протидії витоку інформації. Дається визначення поняттю морфологічного аналізу в DLP-система та аналізується актуальність проблеми забезпечення інформаційної безпеки в сучасному світі з постійним розвитком цифровізації. Досліджуються проблеми та особливості морфологічного аналізу враховуючи особливості різних мов. У зв'язку з особливостями української та російської мови, які найчастіше використовуються в нашому інформаційному просторі, і наявністю великої кількості слів винятків в них, здійснення морфологічного аналізу може бути ускладнене. Для подолання цих труднощів існує можливість вибору методу морфологічного аналізу. У статті алгоритми морфологічного аналізу текстової інформації порівнюються за основними характеристиками, зокрема точність визначення слова при морфологічному аналізі, можливість алгоритму до самонавчання, а також часові затрати на впровадження і налаштування того чи іншого методу в робочу діяльність компанії. Описані переваги та недоліки різних підходів до реалізації, наведені структурні особливості алгоритмів стемінгу - який полягає у виокремленні основної частини слова без закінчення та суфіксу, а не тільки у виділенні кореня, їх приклади та програмні рішення, які доступні на ринку.*

Ключові слова: *DLP-система, морфологічний аналіз, запобігання витоку інформації, алгоритми стемінгу, інформаційна безпека.*

RESEARCH OF MORPHOLOGICAL ANALYSIS ALGORITHMS IN DLP-SYSTEMS TO PREVENT INFORMATION LEAKAGE

Artem Blyzniuk . *State University of Intellectual Technologies and Communication, Kyiv,Ukraine. blizniykartem@gmail.com*

Abstract: *The article investigates the use of morphological method of text information analysis in information leakage control systems. The concept of morphological analysis in DLP-systems is defined and the relevance of the problem of information security in the modern world with the constant development of digitalization is analyzed. The problems and features of morphological analysis are investigated taking into account the peculiarities of different languages. Due to the peculiarities of the Ukrainian and Russian languages, which are most often used in our information space, and the presence of a large number of exception words in them, the implementation of morphological analysis can be complicated. To overcome these difficulties, it is possible to choose a method of morphological analysis. In this article, the algorithms of morphological analysis of text information are compared by the main characteristics, in particular, the accuracy of word detection in morphological analysis, the ability of the algorithm to self-learn, as well as the time required to implement and configure a particular method in the company's work. The advantages and disadvantages of different approaches to implementation are described, the structural features of stemming algorithms - which consists in isolating the main part of the word without ending and suffix, and not only in isolating the root, their examples and software solutions that are available on the market are given.*

Key words: *DLP-system, morphological analysis, information leakage prevention, stemming algorithms,*
information security.

Вступ

Розвиток інформатизації та цифровізації сучасного постіндустріального суспільства, де переважає інноваційний сектор з високопродуктивною економічною системою, все частіше стикається з новою глобальною проблемою, а саме – проблемою інформаційної

безпеки. Левова частка інтересів підприємства визначається інформаційним середовищем в якому воно знаходиться. Тому коли середовище змінюється це також має вплив на інтереси підприємства, зокрема такі зміни можуть становити реальну загрозу майбутній діяльності підприємства.

Необхідно зазначити, що в довідниковій літературі відсутній єдиний погляд на поняття «інформаційна безпека підприємства», що є вкрай актуальним питанням на етапі розвитку і вдосконалення сфери ІТ, яке супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Масштаби дистанційної та віддаленої роботи дають змогу як кіберзлочинцям, так і інсайдерам набагато більше можливостей для крадіжки інформації. Великі ризики можуть бути пов'язані з використанням так званих "тіньових ІТ" (Shadow IT), тобто інформаційних сервісів, що реалізовані на зовнішніх, не корпоративних ресурсах, власники яких не несуть ніякої відповідальності за інформацію, що обробляється.

Використання великих обсягів конфіденційної та "чутливої" інформації, ставить перед відділом забезпечення інформаційної безпеки чи кібербезпеки комплексну задачу для забезпечення належного функціонування компанії, запобігання витоків інформації, розмежування доступів відповідно до посадових обов'язків. Все це значною мірою впливає на впровадження та апробацію такої системи, як DLP.

Виконання досліджень

Обійтись тільки адміністративними мірами для запобігання ІТ-інцидентів, пов’язаних із витоком інформації, на сьогоднішній день вже не вдається. Справа тут не тільки в збільшенні обсягів та різноманіття цінної інформації, а в принциповій відкритості інформаційних систем фінансових установ.

На рис. 1 зображено графік з порівнянням частки витоку інформації за різними типами даних. Лідируючим типом стабільно є персональні дані, близько восьмидесяти відсотків пов'язані з викраденням або ненавмисним розкриттям персональних даних.

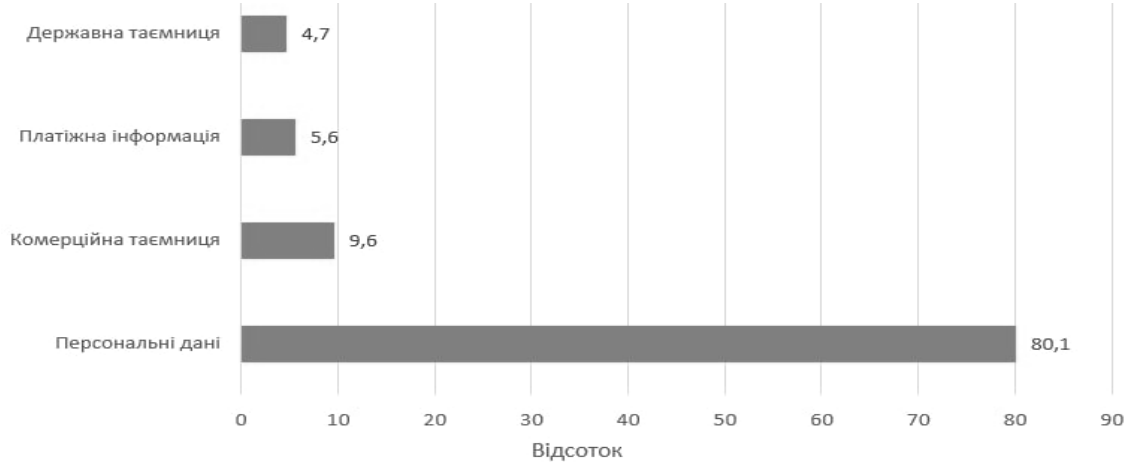


Рис. 1. Графік порівняння витоку інформації за різними типами даних

Основним каналом витоку інформації залишається мережа та електронна пошта, що також вказує на необхідність захисту конфіденційної та персональної інформації, зокрема з використанням DLP-систем.

Якщо порівнювати сфери, де найчастіше трапляються витоки інформації, то перше місце стабільно за останні роки займає індустрія високих технологій, як у західних країнах так і у країнах колишнього СНД.

Через досить високу інформатизацію та діджиталізацію систем у країнах Європи та США на другому місці посідає медичний сектор. Персональні дані пацієнтів, інформація про страхові поліси є конфіденційною, але часто не достатньо захищеною.

Також слід зауважити, що значна частина, а саме 51,2%, порушень та випадків витоку інформації була скоєна персоналом та керівниками компаній. Тому в умовах пандемії та віддаленої роботи працівників компанії та підприємств питання захисту інформації стає ще більше актуальним.

Основою виявлення витоків інформації в сучасних DLP-системах є морфологічний аналіз текстів. Головною перевагою цієї технології є універсальність алгоритмів аналізу, які дозволяють проводити оцінку як повідомлень в різних месенджерах, так і тексту електронних документів. Також перевагами використання цього методу є можливість працювати з вмістом, здатність до навчання лінгвістичного алгоритму, масштабованість і простота налаштування. До недоліків можна віднести залежність від мови, яка використовується, і необхідності застосування імовірнісного підходу.

Морфологічний аналіз являє собою процес визначення граматичного значення словоформи і виділення її основи, або, інакше кажучи, виділення ключових слів у текстовому потоці. Кожен алгоритм морфологічного аналізу складається з двох основних складових - декларативної і процедурної. При цьому декларативна складова являє собою таблиці структурованих даних, необхідних для аналізу, а процедурна компонента містить безпосередньо алгоритми аналізу і допоміжні процедури.

У зв'язку з особливостями української та російської мови і наявністю великої кількості слів винятків в них, здійснення морфологічного аналізу може бути ускладнене. Для подолання цих труднощів існує можливість вибору методу морфологічного аналізу, серед яких найбільш відомими є три основних.

Першим методом є складання морфологічного словника для конкретного підприємства вручну, враховуючи всі ключові слова, які здатні будь-яким чином вказати на витік інформації. Вищеописаний спосіб слід використовувати, коли в наявності відносно невелика множина ключових слів, аналізуючи корінь цих слів. Якщо інформаційна система підприємства (організації) складна, містить велику кількість різноманітних ресурсів, то використання даного методу буде ускладнене, особливо на початкових етапах.

Особливістю другого методу є використання алгоритму стемінгу (англ. stemming), який полягає у виокремленні основної частини слова без закінчення та суфіксу, а не тільки у виділенні кореня. Трапляється, що результати стемінгу можуть бути схожі на визначення кореня слова, проте алгоритм цього методу використовує інші правила та принципи. Тому слово після обробки алгоритмом стемінгу (стематизації) може відрізнятися від морфологічного кореня слова.

Стемінг досить часто використовується в лінгвістичній морфології та для інформаційного пошуку. Багато пошукових систем застосовують цей алгоритм для встановлення синонімічних зв’язків, якщо в них збігаються форми після стемінгу. Для української та російської мови найбільш популярними алгоритмами стемінгу є:

- алгоритм стемінгу Портера;
- Stemka;
- Mystem;
- визначення слова по його суфіксу і афіксу.

Алгоритм стемінгу Портера, інакше званий "Snowball", був розроблений в 1979 році спочатку для англійської мови (тепер фактично стандартний алгоритм стематизації для англійської мови), згодом адаптований під аналіз на основі слов'янських мов. При використанні даного алгоритму стемінг відбувається через ряд правил на основі безлічі існуючих суфіксів і закінчень, які відсікаються. При цьому цей алгоритм не використовує безпосередньо базу основ слів. Для будь-якої мови спочатку необхідно визначити який клас закінчень, має слово, що перевіряється, за допомогою спеціальних правил. Для української мови закінчення матимуть такий вигляд:

- якщо слово іменник воно матиме одне із закінчень а|ев|ов|е|ями|ами|еи|и|ей|ой|ий|й|иям|ям|ием|ем|ам|ом|о|у|ах|иях|ях|ы|ь|ию|ью|ю|ия|ья|я|і|ові|ї|ею|єю|ою|є|еві|ем|єм|ів|їв|\'ю;
- якщо слово відноситься до дієслів, то матиме одне із закінчень сь|ся|ив|ать|ять|у|ю|ав|али|учи|ячи|вши|ши|е|ме|ати|яти|є;
- для дієприкметників закінчення відповідно ий|ого|ому|им|ім|а|ій|у|ою| ій|і|их|йми|их;

- для прикметників закінчення ими|ій|ий|а|е|ова|ове|ів|є|їй|єє|еє|я|ім|ем| им|ім|их|іх|ою|йми|іми|у|ю|ого|ому|ої;

- для дієприслівників закінчення ив|ивши|ившись.

У тому числі перевіряються словотвірні частини, а також частини слова після першої голосної літери, або кінець слова, що не містить голосних.

Після зчитування слова всі літери конвертуються в нижній регістр, після чого перевіряється наявність апострофа та літери "ґ" у слові та видаляються при наявності. Після цього аналізуються закінчення слова у відповідності до частин мови та видаляються при їх наявності. Якщо слово в закінченні має голосну літеру – вона також видаляється. В кінці аналізуються суфікси найвищого ступеню порівняння прикметників, подвоєння, чи є у слові м'який знак та видаляються при їх наявності, а у подвоєнні – одна із літер.

В результаті виконання алгоритму створюється необхідна для впізнання частина слова. Основною перевагою алгоритму стемінгу Портера є відсутність словників основ, що істотно підвищує швидкодію. Часові витрати на роботу алгоритму наведені на рисунку 2.2. Також слід зазначити, що програмна реалізація даного підходу класифікатора не потребує великих обсягів пам'яті на дисковому просторі.

До негативних властивостей даного алгоритму можна віднести можливість втрати частини інформації з аналізованого слова. Крім того, вразливістю даного алгоритму є можливість помилки з боку оператора, що задає правила перевірки.

"Stemka" - російсько-український ідентифікатор морфології, який був створений за допомогою спеціально розробленого морфологічного модуля. Алгоритм заснований на ймовірнісній моделі. Складається масив даних, який включає в себе пари - дві останні букви основи та суфікс, таким чином, виходять моделі різних слів. Після цього визначається ймовірність появи моделей в тексті, і при ймовірності 1/10000 модель відсікається. Результат являє собою таблицю переходів кінцевого автомату, за якими сканується слово.

Для розглянутих алгоритмів "Snowball" і "Stemka" в процесі налагодження було сформульовано правило, яке передбачає наявність хоча б однієї голосної букви в основі.

Mystem був розроблений в 1998 Іллею Сегаловіч. Модель будується в вигляді лісу інвертованих префіксних дерев суфіксів і інвертованого префіксного дерева для основ, для цього використовується словник з перерахуванням всіх граматичних форм слова.

Алгоритм Mystem, функціонування якого полягає в наступному. Чергове аналізоване слово піддається поділу на основу і суфікс. Такий поділ проводиться програмою на основі вже наявного дерева суфіксів. Далі відбувається зіставлення вихідної основи з уже наявними в словнику (блок 2) для знаходження відповідностей. Якщо відповідність знайдено, алгоритм закінчує роботу, і результатом є гіпотеза для словникового слова. Якщо ж відповідність знайти не вдалося, то алгоритм продовжує роботу з пошуку потрібної гіпотези. Для цього відбувається генерація гіпотетичної моделі слова, що базується на основі слова, суфікс і найближчій основі з наявного словника (блок 3).

Після цього отримана модель знову звіряється зі словником. При позитивному результаті алгоритм закінчує роботу. Якщо результат знову негативний і збіг не знайдено, то алгоритм продовжує виробляти вищевказані дії, поступово зменшуючи основу на одну букву (блок 4) до тих пір, поки основа не буде знайдена, або поки кількість букв не скоротиться до двох.

У цьому випадку відбувається ранжування всіх отриманих в ході роботи алгоритму гіпотез (блок 5) по продуктивності і відсікання менш продуктивних. В результаті на виході алгоритму виходить набір гіпотез для неіснуючого в наявному словнику слова. Перевагами даного алгоритму є простота реалізації і словників, а також можливість визначення форм слова, яких не було в словнику. До недоліків цього алгоритму можна віднести те, що хоча алгоритм і працює з українською мовою, проте більш орієнтований на російську.

Четвертим методом є визначення слова по його суфіксу і афіксу, та приведення слова до його початкової форми. Даний спосіб є найбільш раціональним завдяки особливостям слов'янських мов, однак для підвищення якості роботи алгоритму необхідно додати якомога більше слів-винятків. Таким чином, використання одного з перерахованих вище

алгоритмів морфологічного аналізу дозволяє розпізнати конфіденційну інформацію в потоці інформації, що перехоплюється.

Існує кілька критеріїв, що впливають на вибір алгоритму морфологічного аналізу для DLP-систем. До них відносять:

- точність визначення слова при морфологічному аналізі;
- здатність до навчання;
- часові витрати на налаштування системи.

Згідно з дослідженнями точність визначення повинна бути не нижче 95 97%. Здатність до навчання дозволяє зімітувати на етапі налаштування системи небезпечні ситуації, тим самим дозволивши системі самостійно адаптуватися під необхідні параметри, що істотно скорочує час введення системи в експлуатацію.

Для співробітника, що не має навичок аналітика, створення словника для морфологічного аналізу може зайняти досить багато часу, що істотно позначиться на швидкості введення системи в експлуатацію.

Порівняння алгоритмів морфологічного аналізу, що використовуються в DLP-системах, наведені в табл. 1.

З огляду на дані, що представлені в таблиці, найбільш оптимальним алгоритмом морфологічного аналізу для використання в DLP-системах є алгоритм Mystem. Незважаючи на тривалість налаштування, алгоритм має найвищу з перерахованих алгоритмів ймовірність правильного визначення слова і має важливу здатність до навчання.

Таблиця1.

Порівняння алгоритмів морфологічного аналізу

Назва алгоритму	Точність визначення слова при морфологічному аналізі	Можливість до навчання	Часові затрати на налаштування
Складання морфологічного словника	80–85%	-	1–2 дні
Алгоритм стемінгу Портера;	85–90%	-	3–5 годин
Визначення по суфіксу і афіксу	90–96%	-	1–2 дні
Mystem	92–97%	+	2–3 дні
Stemka	87–95%	+	1–1,5 дні

Висновки

DLP продукт виконує функціонал аналіз та моніторингу вихідного трафіку, аналізу інформаційних потоків за декількома технологіями, глибокого аналізу змісту інформації, автоматичний захист конфіденційних даних у кінцевих інформаційних ресурсах, на рівні шлюзів, що передають дані, і в системах, що зберігають дані статично.

Було проведено дослідження методи, які використовує DLP-система для морфологічного аналізу текстових даних в інформаційних системах, проаналізовані різні алгоритмічні підходи для розв'язання труднощів, що пов'язані з особливостями мов.

Визначено, що найбільш оптимальним алгоритмом морфологічного аналізу для використання в DLP-системах є алгоритм Mystem. Незважаючи на тривалість налаштування, алгоритм має найвищу з перерахованих алгоритмів ймовірність правильного визначення слова і має важливу здатність до навчання.

Література

1. Метод стемінгу україномовних текстів для класифікації документів на базі алгоритму Портера. URL: https://clck.ru/UzvxN.
2. Використання адаптованої DLP-системи для блокування витоків інформації. URL: https://cyberleninka.ru/article/n/ispolzovanie-adaptirovannoy-dlp-sistemy-dlya-blokirovaniya-utechek-informatsii/viewer.
3. DLP у документах. URL: https://mirobase.com/spravka/64/.
4. Технології захисту конфіденційної інформації від внутрішніх загроз. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50925/8_s_78-88.pdf?sequence=1.
5. Morphological box of the DLP, 2022. URL: https://www.researchgate.net/figure/Morphological-box-of-the-DLP_fig1_330727964.

References

1. Metod stemingu ukraïnomovnih tekstiv dlya klasifikacií dokumentiv na bazi algoritmu Portera. [A method of stemming Ukrainian-language texts for document classification based on Porter's algorithm]. URL: https://clck.ru/UzvxN.
2. Vikoristannya adaptovanoï DLP-sistemi dlya blokuvannya vitokiv informacií. [Using an adapted DLP system to block information leaks]. URL: https://cyberleninka.ru/article/n/ispolzovanie-adaptirovannoy-dlp-sistemy-dlya-blokirovaniya-utechek-informatsii/viewer.
3. DLP u dokumentah. [DLP in documents]. URL: https://mirobase.com/spravka/64/.
4. Tehnologiï zahistu konfidencijnoï informacií vid vnutrishnih zagroz. [Ttechnologies for protecting confidential information from internal threats]. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50925/8_s_78-88.pdf?sequence=1.
5. Morphological box of the DLP. URL: https://www.researchgate.net/figure/Morphological-box-of-the-DLP_fig1_330727964.

УДК 004.75

АВАРІЙНЕ ВІДНОВЛЕННЯ У ХМАРНИХ МЕРЕЖАХ. ПРОБЛЕМАТИКА WARM СЦЕНАРІЮ АВАРІЙНОГО ВІДНОВЛЕННЯ

DOI 10 36994 / 2788- 5518- 2022-02-04-17

Демидов А.С. *Відкритий міжнародний університет розвитку людини «Україна»,Київ,Україна. anton89d@gmail.com*

Даценко І.П. *Національний Університет Міністерства Оборони України, Київ, Україна. docik_ivan@ukr.net*

Анотація*: Стаття призначена аналізу сучасного стану хмарних систем та сценаріїв аварійного відновлення у хмарах. Проведено аналіз сценарію аварійного відновлення за warm моделлю на прикладі хмарного сервісу розгорнутого у хмарі AWS. Визначені основні проблеми, які приводять до збільшення RTO (recovery time objective). Запропоновані рекомендації щодо зменшення затримки відновлення сервісу після відмови.*

Ключові слова*: хмара, хмарні провайдери, AWS, RTO, аварійне відновлення*

DISASTER RECOVERY IN CLOUD. PROBLEMS OF WARM DISASTER RECOVERY SCENARIO

Anton Demydov*. Open International University of Human Development "Ukraine", Kyiv, Ukraine. anton89d@gmail.com*

Ivan Datsenko. *National Defense University of Ukraine, Kyiv, Ukraine**.** docik_ivan@ukr.net*

Abstract: *Cloud computing is the current routine of using Information Technologies all over the world. This concept is evolving, large cloud computing providers adding more and more functionality, becoming one of the most popular and fastest-growing technologies in the IT field. Disaster recovery is a constant problem in the information technology sphere, but the problem is much broader for cloud providers because they must continue to provide service to customers even during disasters. An accident is an unforeseen event during the system's lifetime. This can be caused by natural disasters, hardware or software failures, human error, or sabotage. This can lead to serious financial losses from a business point of view. For a business, the main purpose of having a disaster scenario is business continuity, which means restoring online services after a failure. The disaster recovery scenario should cover multiple levels of restoring – the data layer, the system layer, and the program layer. There are 3 main approaches of disaster recovery scenarios. Hot model – physical mirroring of infrastructure. Warm model – partial mirroring. Cold model – backups are usually stored outside of the cloud computing provider. A warm model is preferable for medium and small businesses because of its price and complexity. The paper compares different disaster recovery scenarios, their advantages, and disadvantages, and specifies possible problems and high-level solutions for the warm model. Reviewed a real case service deployed to Amazon Web Services provider. Highlighted the need of using Infrastructure as a code to have the ability to change infrastructure as quickly as possible and provided recommendations for decreasing RTO and RPO by using additional load balancers, DNS failover, and PostgreSQL bi-directional replication.*

Key words*: Disaster Recovery, Cloud, AWS, RTO, Warm mo*del

Вступ

Сьогодні попит на послуги провайдерів хмарних обчислювань зростає з великою швидкістю. За оцінкою Fortune ринок досяг значення 480.04 міліардів доларів у 2020 році[1], хоча у 2020 році був на рівні 222 міліардів доларів. З дослідження Gartner хмарні обчислення є однією з десяти найбільших інновацій у сфері інформаційних технологій. [2]

Попередні дослідження стверджують, що хмарні обчислення є формою конвергенції двох основних тенденцій в інформаційних технологіях[3]:

- IT – ефективність, за якою підприємства можуть використовувати сучасні комп'ютерні системи за допомогою високомасштабованих апаратних і програмних ресурсів
- Бізнес – гнучкість, за якою IT використовуються як конкурентна перевага завдляки швидкому розгортанню та співпраці з клієнтами в реальному часі.

Технологія хмарних обчислень має низку особливостей, які роблять її можливим вирішенням різноманітних проблем. Наведенм деякі з цих характеристик [4]:

- Масштабованість
- Віртуалізація
- Надійність
- Універсальність
- Еластичність ресурсів
- Вимірюваність послуг на вимогу
- Економічність
- Керованість
- Аварійне відновлення

Національний інститут стандартів та технологій США дає 5[5] основних характерстик які описують провайдерів хмарного обчислення:

1. Самостійне обслуговування (On-demand self-service).
2. Користувач має можливість отримувати ресурси за запитом
3. Швидкісний мережевий доступ
4. Об'єднання ресурсів в пул
5. Швидкодіюча еластичність - швидке отримання та звільнення ресурсів
6. Врахованість послуг

Однією з найбільш важливих тем у хмарних мережах є аварії та аварійне відновлення після. Аварії яки були спричинені людьскою помилкою або природним явищем можуть привести до дорогих збоїв та частковї або повної зупинки бізнесу. На рис.1 ми можемо побачити залежність суми збитків та часу якщо порівнювати традиційни дата центри та провайдерів хмарних обчислювань.

Рис. 1. Орієнтована швидкість відновлювання хмарного сервіса в порівнянні з традиційним дата центром

Хоча провайдери хмарних обчислень наголошують у своїх угодах про надання послуг (SLA) на доволі високих рівнях доступності сервісів - аварії бувать і у них. Більш того, бізнес потребує мати

сценарій відновлення сервісу у випадку аварії. Можно виділити наступні сценарії які повинні тестуватися:

1. Втрата даних і відновлення резервної копії. Речі, які слід враховувати:
    a. Час, який займе відновлення.
    b. Непередбачувані проблеми під час відновлення.
    c. Потенційні способи покращення часу відновлення.
2. Невдале резервне копіювання. Необхідно ретельно перевіряти резервні копії і проводити тестування розгортання з них.
3. Збої в роботі мережі.
4. Збої обладнання.
5. Тестування безпеки.

Існує декілька підходів для розробки сценарію аварійного відновлення. Усі вони базуються на патерні використання системи та стратегіях резервного копіювання та резервування. Наприклад, резервування використовує статегію роботи паралельної інфраструктури, яка працює у іншому регіоні.

У таблиці ми можемо бачити орієнтований час та швидкість аварійного відновлення та його можливі сценарії.

Таблиця 1.
Моделі аварійного відновлення

Модель	Час синхронізації	Час відновлення	Характеристики резервного копіювання
Гаряча (Hot)	Секунди/Хвилини	Хвилини	Фізичне відзеркалення інфраструктури
Тепла (Warm)	Години	1-24 години	Обмежене фізичне/віртуальне відзеркалення
Холодна (Cold)	Дні	Більше 24 годин	Резервне копіювання поза провайдером хмраного обчислення

Основним завдання розробки сценарію аварійного відновлення – мінімізування проміжку часу від збою до відновлення сервісу – RTO (recovery time objective). Затримки відновлення після відмови складаються з [2]:

- Часу, необхідного на налаштування обладнання
- Час ініціалізації операційної системи
- Час ініціалізації програмного продукту
- Час відновлення стану даних
- Мережеві затримки (IP, DNS)

Показниками ефективного сценарію є мінімальність впливу на нормальну роботу сервіса, географічне розділення та безпековий компонент.

Малі та середні бізнеси, які можуть собі дозволити невеликий час простою у разі аварії віддають перевагу Warm моделі аварійного відновлення.

У статті розглядається реальний кейс використання Warm моделі аварійного відновлення у хмарі Amazon Web Services. Сервіс використовує різноманітні можливості хмари. Основною базою даних є RDS PostgresSQL. Метою дослідження є надання рекомендацій щодо зменшення часу відновлення системи після аварії у іншому географічному регіоні.

Виконання досліджень

Дослідження проводилося на реальному програмному продукті, розгорнутому в хмарі AWS у географічному регіоні us-east-1 (N. Virginia). Піддослідний програмний продукт має мікросервісну архітектуру та використовує наступні хмарні сервіси:

- Elastic Container Service – сервіс для оркестрації програмних продуктів з мікросервісною архітектурою
- Elastic Container Registry – сервіс для зберігання контейнерів
- AWS RDS – сервіс баз даних. Даний програмний продукт використовує Postgres
- AWS Dynamo DB – глобальна NoSQL база даних
- AWS EC2 – сервіс віртуальних машин
- AWS S3 –об'єктно-орієнтований сервіс для зберігання даних
- AWS Lambda – безсерверний, керований подіями обчислювальний сервіс, який дозволяє виконувати код практично для необмеженого типу програми або сервісу без надання серверів та можливості їх безпосереднього обслуговування
- AWS API Gateway – сервіс, призначений для створення, публікації, обслуговування, моніторингу та забезпечення безпеки API у будь-яких масштабах
- Як ми бачимо на рис. 2, усі запити від клієнтів сервіса надходять на Application Load Balancer котрий розподіляю навантаження та виконує функціїї SSL Termination. Основний програмний продукт розгорнуто за допомогою AWS Elastic container service котрий виконує функцію оркестрації контейнерів. Дані зберігаються у декількох базах даних - AWS Dynamo DB та AWS RDS Postgres. Також, є декілька API сервісів, які використовують AWS Lambda та AWS API Gateway. У якості брокера повідомлень використовується RabbitMQ, який розгорнутий за допомогою auto-scaling групи на віртуальних машинах EC2. Додамо, що вся інфраструктура розгорнута за допомогою моделі Infrastructure as a Code та програмного продукта Terraform. Він дозволяє декларативно курувати інфраструктурою, що дає можливість її менеджменту у будь який час, змінюючи лише декілька змінних. Наприклад, ось як декларується Application Load Balancer:

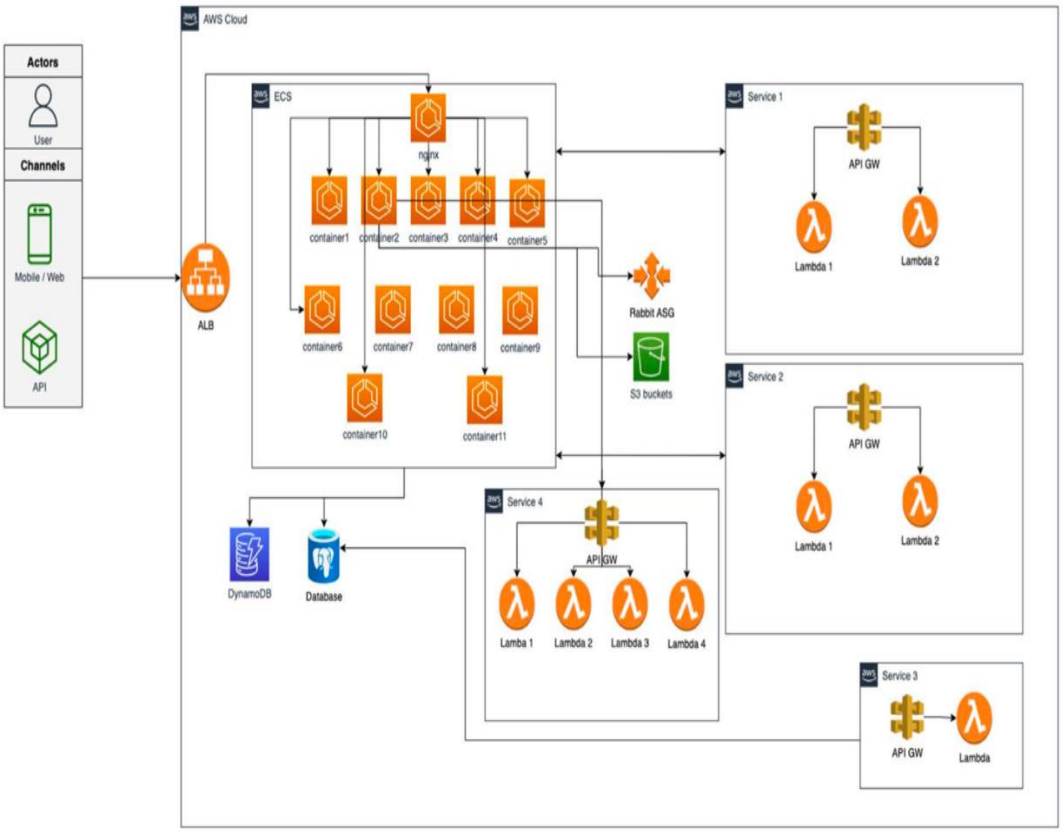


Рис. 2. Інфраструктурна діаграма

```
resource "aws_alb" "vcc-proxy-alb" {
  name               = "${local.env}-${local.application}" # Naming our load balancer
  load_balancer_type = "application"
  subnets            = data.aws_subnets.public.ids
  # Referencing the security group
  security_groups = [aws_security_group.vcc-proxy-alb-sg.id]
}
resource "aws_lb_target_group" "vcc-proxy-alb-tg" {
  name        = "tg-${local.env}-vcc-proxy"
  port        = 80
  protocol    = "HTTP"
  target_type = "ip"
  vpc_id      = data.aws_vpc.vpc.id
  health_check {
    matcher = "200,301,302"
    path    = "/api/health-check/"
  }
  depends_on = [aws_alb.vcc-proxy-alb]
}
resource "aws_lb_listener" "alb-listener" {
  load_balancer_arn = aws_alb.vcc-proxy-alb.arn # Referencing our load balancer
  port              = "443"
  protocol          = "HTTPS"
  ssl_policy        = "ELBSecurityPolicy-2016-08"
  certificate_arn   = local.cert_arn
  default_action {
    type = "fixed-response"
    fixed_response {
      content_type = "text/plain"
      message_body = "hello"
      status_code  = "200"
    }
  }
}
resource "aws_lb_listener" "alb-listener-redirect" {
  load_balancer_arn = aws_alb.vcc-proxy-alb.arn
  port              = "80"
  protocol          = "HTTP"

  default_action {
    type = "redirect"

    redirect {
      port        = "443"
      protocol    = "HTTPS"
      status_code = "HTTP_301"
    }
  }
}


resource "aws_lb_listener_rule" "redirect-to-vcc-proxy" {
  listener_arn = aws_lb_listener.alb-listener.arn
  action {
    type             = "forward"
    target_group_arn = aws_lb_target_group.vcc-proxy-alb-tg.arn
  }
  condition {
    host_header {
      values = ["${local.proxy_domain}.com"]
    }
```

```
  }
}
```

Щодо можливих змін – усе конфігурується у файлі variables.tf, що дає можливість визначити скільки ресурсів має той чи інший географічний регіон, вносити зміни у версіях тощо.

Базуючись на можливих сценаріях аварійного відновлення та вимогах бізнесу для даної системи була обрана Warm модель сценарію аварійного відновлення. У іншому географічному регіоні була розгорнута така сама архітектура, за допомогою коду terraform. Для зменшення витрат бізнесу інфраструктура у іншому регіоні має вдвічі менше ресурсів, тобто кількість працюючих контейнерів, розмір бази даних.

Для резервування бази даних був використаний механізм read-replica, який дозволяє мати репліку бази даних у іншому регіоні, яка доступна тільки на читання. (рис 3)

Зазначимо, що версії програмних продуктів мають бути оновлені до тих самих версій, які є у основного стеку. Це може бути досягнено за допомогою CI/CD принципа та постійного моніторингу. У випадку аварії, інженери, які відповідають за інфраструктуру повинні отримати дозвіл на ініціювання аварійного сценарію. Якщо такий дозвіл є, то вони повинні виконати наступні кроки:

- Ініціювання репліки бази даних як основної
- Заміна записів DNS для усіх сервісів, які використовуються у даній системі
- Моніторинг журналів логування резервної системи та збільшення кількості ресурсів за умов великого навантаження та правильної роботи.
- При обранні WARM сценарію аварійного відновлення ми можемо
- мати доволі швидке переключення DNS записів, але для деяких
- клієнтів це може стати проблемою, якщо вони використовують власні
- DNS сервера з великим часом кешування. Тому, TTL DNS записів має
- бути доволі малим. Але, основною проблемою є затримка реплікації
- бази даних між географічними регіонами (рис. 4).
- При моделюванні аварії у даній конкретній системі ми можемо стверджувати, що у випадку аварійного сценарію час на відновлення програмного стеку у іншому географічному регіоні може коливатися від 45 хвилин до декількох годин. Зведемо дані у таблицю:

Таблиця 2.
Час ініціювання аварійного стеку

Сервіс	Час на зміну	Коментарі
DNS записи	1-15 хвилин	Залежить від DNS TTL та кількості DNS записів
Read-Replica Promotion	15-120 хвилин	Залежить від об’єму бази даних та її конфігурації

Це означає, що при аварії є шанс втрачання певної кількості даних. Також, швидкість переключення репліки бази даних до мастера займає значний час.

Для вирішення цих проблем є декілька опцій:

- Використання між регіональних балансувальників нагрузки, які здатні переключати трафік на інший регіон автоматично, або спеціалізованих сервісів, таких як AWS Global Accelerator.
- Використання master-master реплікації бази даних, або bi-directional реплікацію.
- Використання глобальних баз даних.
- Використання контейнеризації для зменшення часу ініціалізації.

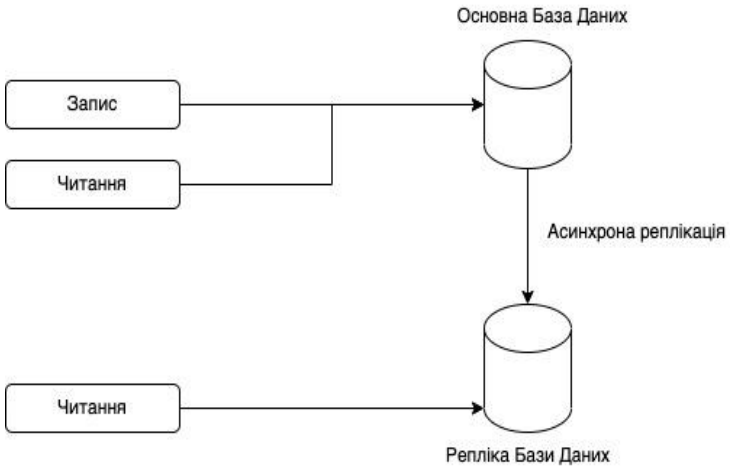


Рис. 3. Реплікація бази даних у інший географічний регіон

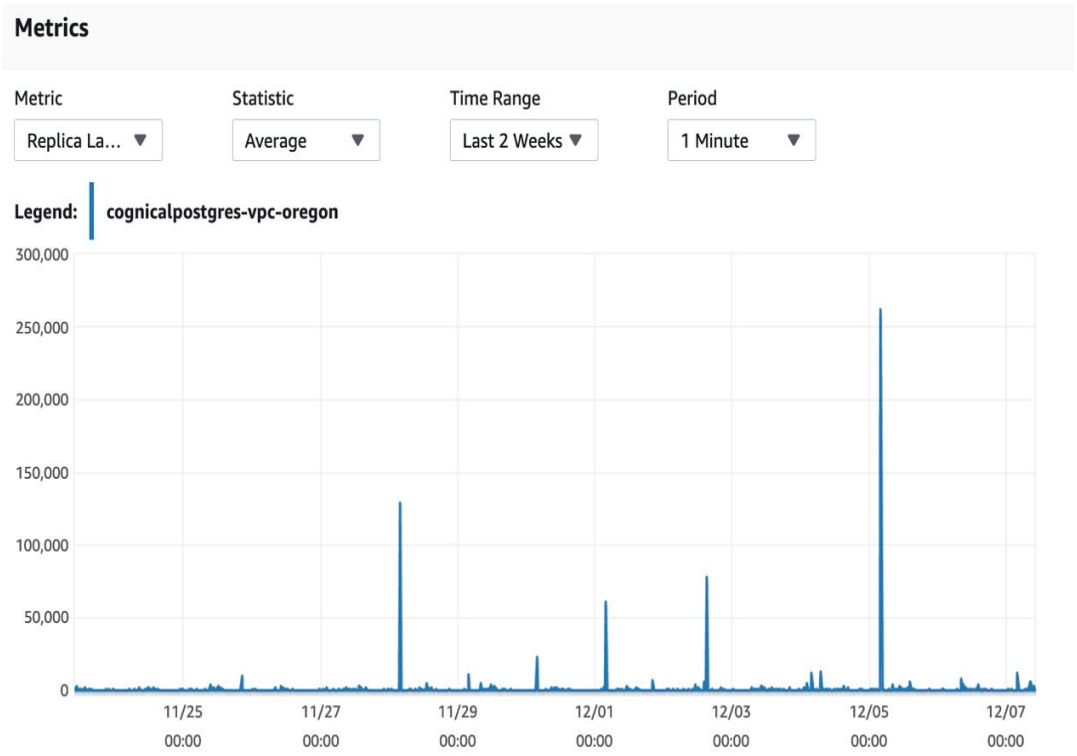


Рис. 4. Затримка реплікації бази даних у інший географічний регіон

Висновки

У статті розглянуті основні сценарії аварійного відновлення у хмарних мережах.

Проведені дослідження проблематики Warm моделі аварійного відновлення на основі працюючого сервіса, розгорнутого у хмарі AWS.

Основними проблемами, які збільшують час відновлення сервісу після аварії є швидкість переключення DNS записів після аварії і швидкість переключення мастера бази даних у інший географічний регіон.

Запропоновані методи оптимізації RTO – використання bi-directional реплікації бази даних, що дозволить мати фактично мастер-мастер реплікацію. Це означає, що буде збережений час, який зараз витрачається на переключення. Також, запропоновано використання між-регіональних балансувальників навантаження, які дозволять зменшити до 0 час переключення DNS записів.

Література

1. Електронний ресурс. Fortubebusinessinsights. Cloud computing Market size, Analysis. URL: https://www.fortunebusinessinsights.com/cloud-computing-market-102697
2. Електронний ресурс. Gartner, “Gartner identifies the top 10 strategic technologies for 2011”, URL: http://www.gartner.com/it/page.jsp?id=1454221
3. Associated Risks of Cloud Computing for SMEs. Open International Journal of Informatics (OIJI), (2012) ,1, pp.37-45.
4. Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010. R. Buyya, J. Broberg, and A. Goscinski, “Cloud Computing Principles and Paradigms”, John Wiley & Sons, 2011.
5. Таненбаум Э.. Современные операционные системы. Питер, 2018. 553 ст.

References

1. Fortubebusinessinsights. Cloud computing Market size, Analysis. URL: https://www.fortunebusinessinsights.com/cloud-computing-market-102697
2. Gartner, “Gartner identifies the top 10 strategic technologies for 2011”, URL: http://www.gartner.com/it/page.jsp?id=1454221
3. Associated Risks of Cloud Computing for SMEs. Open International Journal of Informatics (OIJI), (2012) 1, pp.37-45.
4. Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010. R. Buyya, J. Broberg, and A. Goscinski, “Cloud Computing Principles and Paradigms”, John Wiley & Sons, 2011
5. Tanenbaum E. Sovremennye operacionnye sistemy. [Modern operating systems]. Piter, 2018. 553 s.

УДК 004.624, 004.633, 004.632.4

МОБІЛЬНИЙ ПРИСТРІЙ ЯК ЧАСТИНА АДАПТИВНОЇ КЕЙС-МЕНЕДЖМЕНТ СИСТЕМИ

DOI 10 36994 / 2788- 5518- 2022-02-04-18

Бровченко Є. М. *Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. yebrovchenko@hotmail.com*

Самарай В. П.*, к.т.н.,доц. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. samaraj@ukr.net*

Даценко І. П.*, к.т.н. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. docik_ivan@ukr.net*

Павленко В. І.*, к.ф.-м.н.,доц. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. pavlenko.v@i.ua*

Анотація: *У статті розглядається проблема використання мобільних пристроїв як частини адаптивної кейс-менеджмент системи (від англ. Adaptive Case Management, Dynamic Case Management, Advanced Case Management), захист та обробка неструктурованої інформації на мобільних пристроях що активно використовуються в адаптивних кейс-менеджмент системах. Особливості використання та потенційні проблемні моменти в інтеграції та взаємодії.*

Ключові слова: *Мобільний пристрій; смартфон; адаптивний кейс-менеджмент; структуровані та не структуровані дані; найкращі практики взаємодії користувача з мобільним пристроєм та ACM;*

MOBILE DEVICE AS PART OF AN ADAPTIVE CASE MANAGEMENT SYSTEM

Evgen Brovchenko, *Open International University of Human Development "Ukraine", Kyiv, Ukraine. yebrovchenko@hotmail.com*

Valery Samarai*, Ph.D., Ass.Prof.Open International University of Human Development "Ukraine", Kyiv, Ukraine. samaraj@ukr.net*

Ivan Datsenko, *Ph.D. Open International University of Human Development Ukraine", Kyiv, Ukraine. docik_ivan@ukr.net.*

Volodymyr Pavlenko, *Ph.D.,Ass.Prof. Open International University of Human Development "Ukraine", Kyiv, Ukraine. pavlenko.v@i.ua*

Abstract: *The article considers the problem of protection and processing of unstructured information on mobile devices that are actively used in adaptive case management systems. Peculiarities of use and potential problem points in integration and interaction. In modern conditions of uncertainty and rapidity, the success of solving tasks or problems in many cases depends on effective response to certain circumstances and established business processes. Therefore, adaptive case management (Adaptive Case Management, Dynamic Case Management, Advanced Case Management) is a concept of dynamic management of business processes. ACM systems are designed for solving problems of collective interaction, setting tasks and assignments, and monitoring performance. The possibility of accumulating corporate knowledge and practices for reuse can also be considered a significant advantage. The main idea of the adaptive case management system is the dynamic management of business processes in conditions of uncertainty and the requirement for self-adjustment. It should be noted separately that the user participates not only in the process of solving the tasks, but also the opportunity to influence the development of the system. The channels of interaction in the system can be noted as the next important element. The development of digital technologies has given us the opportunity to use mobile devices in many areas of our lives. ACM systems were no exception. Apparently, a mobile device can be seen everywhere today, so it is not*

surprising that it can occupy a separate important place in ACM systems. This device may have several advantages and unique features. This creates both convenience for users and problems. The security of using mobile devices has always been a priority issue. The use of mobile downtime in modern human life and the functionality of mobile platforms require certain security measures in the context of data storage. More and more private information is entering digital display and uncontrolled use. The development of the industry requires fast, reliable, and effective solutions that fall not only in the economic plane, but also in the plane of cyber security.

Key words: *Mobile device; Adaptive Case Management, ACM; security; data protection; UI/UX; structured and unstructured data; mobile user experience and ACM best practices.*

Вступ

В сучасних умовах невизначеності та швидкоплинності успіх вирішення поставлених задач чи проблем в багатьох випадках залежить від ефективного реагування на певні обставини та встановлені бізнес-процеси. Особливо це важко зробити коли заздалегідь ви не маєте повної картини та чіткої постановки задачі чи проблеми, формалізація теж не завжди може мати бажані результати. Тому й не дивно що виникає логічне питання а що з цим робити. Однім з можливих рішень в цьому напрямку можуть бути кейс-менеджмент (від англ. Case Management, CM). Отже, кейс-менеджмент – це алгоритм, в якому один етап послідовно змінює інший, від виявлення основних вимог до кінцевої стадії розв'язання початкової задачі. Якщо цей алгоритм покласти в більш формальну площину то отримаємо кейс-менеджмент систему.

Отже адаптивний кейс-менеджмент (від англ. Adaptive Case Management, Dynamic Case Management, Advanced Case Management) – це концепція динамічного управління бізнес-процесами. Системи ACM призначені для вирішення задач колективної взаємодії, постановка задач та доручень, контроль за виконанням. Також суттєвою перевагою можна вважати можливість накопичення корпоративних знань та практик для повторного використання.

Власне основна ідея адаптивної кейс-менеджмент системи це динамічне управління бізнес процесами в умовах невизначеності та вимога до само налаштування. Окремо треба зазначити участь користувача не лише в процесі вирішення поставлених задач а й можливість впливати на розвиток системи в цілому.

Наступним важливим елементом можна зазначити власне канали взаємодії в системі. Розвиток цифрових технологій дає нам можливість використовувати мобільні пристрої у багатьох сферах нашого життя. Не винятком стали ACM системи. Мабуть мобільний пристрій можна побачити сьогодні усюди тому й не дивно що цей він може займати окреме важливе місце в ACM системах. Цей пристрій може мати ряд переваг та унікальних можливостей. Власне це й створює як зручності для користувачів так і проблеми. Безпека використання мобільних пристроїв завжди була пріоритетним питанням.

Використання мобільних простоїв в сучасному житті людини та функціональні можливості мобільних платформ вимагають певних заходів безпеки у контексті зберігання даних. Все більше приватної інформації потрапляє в цифрове відображення та не контрольоване використання.

Виконання досліджень

Адаптивна кейс-менеджмент система (ACM), мобільний пристрій та неструктуровані данні**.**

Система ACM дає можливість керувати усіма поточними корпоративними проектами і співробітниками, які беруть в них участь, повністю контролювати виконання проекту на кожному етапі і формувати бібліотеки «кращих практик» в процесі реальної роботи. Враховується досвід та побажання користувачів.

Існує багато думок як можна визначити поняття адаптивний кейс-менеджмент. Деякі експерти переконують, що концепція ACM є альтернативною по відношенню до концепції BPM (англ. Business Process Management, управління бізнес-процесами).

Тобто вона має на меті вирішити ту ж саму задачу ефективної організації бізнес-процесів, але іншими засобами та методами. Різницю в підходах класифікації можна охарактеризувати наступним чином: BPM йде від структури процесів, складу кроків, які необхідно зробити, щоб досягти мети та плавленої задачі. Дані виникають в ході виконання процесу чи задачі, і є повністю залежними від нього. ACM йде від інформації і бізнес-даних, що беруть свій початок власне й використовуються в ході роботи і необхідних для того, щоб вважати результат досягнутим. Тобто процеси виникають в контексті даних, а не навпаки.

Деякі фахівці можуть стверджувати, що ACM - це всього лише спрощена версія BPM, що вирішує ті ж завдання, що і BPM. А існує думка, що ACM - це доповнення до BPM-системи, у якій немає засобів та можливості завантаження файлів, аудіо, відео чи фотографій користувачів, засобів для ведення внутрішніх та зовнішніх дискусій чи діалогів (можливе використання чатів але як частина екосистеми), в той час як для будь-якої ACM ці засоби вважаються стандартними чи навіть базовими. Є група фахівців що стверджують наступне: ACM - це соціальний BPM, в якій наступний крок процесу визначається рішенням людини чи групи людей, що знаходиться в соціальному еко середовищі та мають безпосереднє відношення до процесу. А це як раз ті базові засади, яких не вистачає традиційним BPM-системам. При такому визначені BPM і ACM гармонійно доповнюють один одного, дозволяють автоматизувати як структуровані, усталені бізнес-процеси підприємства чи організації, так і щоденну колективну роботу співробітників чи окремий учасників процесу.

Слід зазначити наступні корисні та цікаві особливості адаптивного кейс-менеджменту.

Система ACM надає можливість накопичення та використання корпоративних знань то досягнень для їх повторного використання чи удосконалення. Успішно завершений кейс, що містить досвід колективної роботи співробітників та учасників, підаєть обробці та редагуванню (для забезпечення універсальності та унікальності) і зберігається в бібліотеці шаблонів для загального використання. Потім, при необхідності, новий кейс на цю тему може бути створений на основі архівної копії чи шаблону.

Адаптивність і гнучкість ACM дозволяє автоматизувати та покращити бізнес-процеси підприємства чи іншої установи в звичному та доступному для співробітників(користувачів) вигляді. Нові кейси формуються самими користувачами як списки завдань та цілей, які потрібно виконати, коригуються і доповнюються по ходу виконання процесу. Причому історія життя того чи іншого кейсу має фіксуватись та запобігати можливим несанкціонованим маніпуляціям.

Простота і соціальність системи ACM дозволяють автоматизувати поточні процеси підприємства(установи, тощо) без детального аналізу чи обробки бізнес-процесів і складного налаштування чи навить виключає необхідність в специфічному програмуванні. Замість складних описів бізнес-процесів ACM використовує схожий підхід контрольних точок, що являють собою список завдань, які необхідно виконати чи розглянути. Під час виконання процесу цей перелік коригується і доповнюється. Ці доповнення можуть бути здійснені будь-яким учасником процесу в залежності від політики доступу та поточного стану кейсу.

Систему ACM можна ефективно використовувати практично негайно після інтеграції, поступово створюючи та вдосконалюючи кейси (послідовності завдань і доручень) на будь-які теми та будь-якою кількістю користувачів

Контролювати виконання проекту на кожному етапі та вносити зміни згідно встановлених правил [1].

Розглянемо функціональні можливості ACM.

Система ACM дозволяє:

Керувати кейсами - наборами задач та доручень, пов'язаних с виконанням цілого чи окремого бізнес-процеса (можливе розбиття). Кейси - послідовність повідомлень, що

містять опис проблеми чи задачі, доручення, дискусії та переписки користувачів, списки виконавців та учасників, файли, форми даних, бізнес-правила, тощо.

Зберігати всю інформацію о бізнес-процесі - документи, фотографії, відеоролики, електроні листи, іншу переписку користувачів, креслення та будь які файли. Треба зазначити що вся вхідна/вихідна інформація маю бути зафіксована в системі за певними правилами.

Адміністрування користувачів, що входять в команду кейса, керувати доступом до задач чи під задач, файлів та повідомлень кейса, повідомляти користувачів о певних подіях та стану кейса в цілому.

Адмініструвати та підтримувати управління правилами та політиками (в тому числі політиками безпеки), що дозволяють автоматично активізувати наступні задачі(крокі) кейсу після закінчення попередніх чи досягнені певних контрольних точок, інформувати користувача, керування архівом.

Вести журнал взаємодії користувача з дорученнями / повідомленнями / кейсом / певним файлом чи повідомленням, коли доручення/повідомлення створюється, редагується чи зміна його статусу.

Підтримувати та проводити модерацію корпоративних дискусійних форумів за різними темами та проектами. Підтримувати бібліотеки шаблонів, процес архівації.

Представляти списки задач в кейсах.

Здійснювати погодження, рецензування та затвердження документів чи інтеграція з системами електронного документа обігу або іншими суміжними системами. Формувати складнопідрядні бізнес процеси у вигляді покрокових інструкцій до виконання.

Як зазначалось, можливим каналом взаємодії та зв’язку в АСМ системі може бути мобільний пристрій чи мобільний телефон. Отже давайте трохи розглянемо це питання. Мобільний пристрій - це термін можна використати для будь-якого портативного комп’ютера що має доступ до мережі то володіє певним рівнем мобільності та незалежності. Також цей термін можна замінити на портативним пристрій, смартфон, смарт-пристрій, маленький комп'ютер. Планшети, будь які електронні сканери, смартфони, кишеньковий комп'ютер, кишеньковий персональний комп'ютер, (КПК) та портативні програвачі з розумними можливостями – це все мобільні пристрої. Окремо можна відділити смартфон. Смартфон - це категорія стільникових телефонів які поєднують функції надання стільникового зв'язку з виконанням широкого спектру додаткових функцій і можливостей, забезпечуваних відкритими операційними системами й додатками до них. Ці пристрої мають ознаки персонального комп’ютера, постійне сховище інформації (як внутрішнє так і зовнішнє), великі об’єми оперативної пам'яті, потужний центральний та графічний процесор, можливість інтеграції з хмарними сервісами чи сховищами.

До переваг можна віднести : компактність, мобільність, доступність, швидкість, сучасність, автономна робота, не великі розміри. Відносно легка модернізація як програмного забезпечення так і апаратного. Можливість використання сучасних інформаційних рішень та технологій.

Мобільні пристрої мають розширенні можливості:

- Отримання, обробка та зберігання голосових викликів. Користувач може в певній мірі проводити налаштування за власним вподобаннями чи обмеженнями.
- Спілкування різними каналами. Це може буде як класичній дзвінок так і велика кількість текстових, аудіо чи відео форматів обміну, починаючи від смс та закінчуючи спеціалізованим програмним забезпеченням.
- Перегляд веб-сторінок. Власне мобільний пристрій може виконувати усі звичайні фікції та використовувати специфічні.
- Геолокація. Визначення місце розташування користувача. Встановлення певних правил чи політик в залежності від координат.

- Біометрія. Сюди можна віднести як розпізнавання обличчя чи голосу так і відбитки пальців.
- Використання електронної пошти, текстових повідомлень та голосової пошти. Взагалі на сьогодні мобільні пристрої до певної міри можуть конкурувати з класичними комп’ютерами з точки зору функціональності.
- Використання фото, аудіо та відео. Можливість використання цих функцій за різними сценаріями.
- Використання віртуальних асистентів, наприклад Siri, Cortana або Google Assistant. В деяких випадках роботу таких систем можна вважати як роботу штучного інтелекту.
- Різноманіття формфакторів, розмірів. Можливість обрати оптимальну конфігурацію з точки зору ефективності та доцільності.
- Бездротова робота. Можливість онлайнової/офлайнової роботи. Кінцевий користувач може створити певний оптимальний шаблон роботи чи користування.

Переважна більшість мобільних пристроїв працюють під керуванням повноцінної операційної системи. Це дає можливість гнучкого та ефективного використання, створення певних навиків роботи та взаємодії з користувачем, створювати складні сценарії взаємодії.

До найпоширеніших операційних системи та платформи можна віднести Android та iOS.

Android - платформа для смартфонів, з відкритим вихідним кодом, що розробляється ОНА (група компаній на чолі з Google). Платформа базується на Linux. В 2012 році за даними IDC ринкова доля цієї мобільної операційної системи склала 75 %.[4]. Загальна відкритість платформи з точки зору розробки та інтеграції розглядається як конкурентна перевага в колах як інженерів так і кінцевих користувачів. Але це відкритість може бути об’єктом зловживань чи шахрайських схем.

iOS - використовується в мобільних пристроях та гаджетах компанії Apple, розробляється та супроводжується на основі Mac OS X.). Друга за популярністю ОС для смартфонів станом на 2019 рік. Вважається що ця операційна система є досить закритою з точки зору сторонньої розробки, власне це й регламентує надійність та стійкість в цілому. Проте це гальмую еволюцію продукту, тому останнім часом ми можемо спостерігати спроби стати відкритою та прозорою платформою.

Треба зазначити що існує багато специфічних та вузько спрямованих мобільних операційних систем. Їх використання переважно спрямовано на прикладні задачі та не має широкого використання. Тому з точки зору АСМ систем ці рішення на мають перспективи.

Однією з переваг цих платформ є можливість розробки та використання програмного забезпечення сторонніми розробниками. Тобто при виконання певних умов зі сторони провайдера послуг будь-хто може створити свою власну програму (мобільний застосунок, додаток) та мати можливість використовувати на платформі, встановленя на самому пристрої або можуть бути завантажені на нього з онлайн-магазинів мобільних застосунків, таких як App Store, Google Play. Наразі розробники мають можливість повної інтеграцію своїх програм з операційною системою, використання усіх функцій мобільного пристрою і гнучку систему управління додатком. Такий уніфікований та формалізований підхід створює додатковий рівень безпеки, гарантує високу якість обслуговування та користування, виробляє певні корисні звички у кінцевого користувача. Ба більше це основа для розвитку галузі.

Також слід акцентувати увагу на можливості адміністрування та керування мобільним пристроєм як на рівні операційної системи так і на рівні окремого додатку. Наприклад є можливість дистанційного адміністрування як мобільного пристрою так і додатку. Управління мобільними додатками (Mobile Application Management, MAM)

описує програмне забезпечення та послуги, відповідальні за надання та контроль доступу до внутрішньо розроблених і комерційно доступних мобільних програм, які використовуються в бізнес середовищах. Управління мобільним пристроєм (Mobile Device Management, MDM) дає можливість здійснювати контроль на рівні мобільного пристрою.

Окремою перевагою мобільних платформ можна вважати доступність та відносно не велику ціну. Як результат є можливість використовувати особистий мобільній пристрій в робочому середовище. Тобто є небезпека використання робочої інформації на не підконтрольній території. Власне існує стратегія, що призначена для компенсації ризику - Bring Your Own Device (BYOD). Коли співробітник чи користувач використовує особистий пристрій в робочому середовище за умови прийняття певних обмежень та правил користування. Керування мобільними додатками чи пристроєм дає змогу корпоративному IT-персоналу використовувати необхідні програми, контролювати доступ до бізнес-даних і видаляти локально бізнес-дані з пристрою, якщо вони втрачені або якщо їх власник не є чистиною компанії.

Контейнеризація є альтернативним підходом до безпеки. Це окремий рівень забезпечення функціональних потреб користувача. Замість того, щоб контролювати весь пристрій співробітника, додатки для контейнерування створюють ізольовані сховища окремо від особистих даних. Контроль компанії над пристроєм поширюється лише на цей окремий контейнер.[5]

Власне що з чим ми маємо справу в кейс-менеджмент системі? Що становить цінність? Це данні. Але не просто данні а не структуровані. Наприклад це може бути аудіо, відео або фото, повідомлення електронної пошти, тощо. Сама ідея ACM системи нам говорить що в якості інформації може бути що завгодно, є можливість навіть не знати й не розуміти про саму суть даних але ми маємо бути готовими до їх використання та вміло керувати. Головна проблема такого роду інформації це невизначеність та складності в аналізі, невідповідність заздалегідь визначеній моделі. Ще й керувати не завжди можна ефективно. Як окрему особливість зазначимо можливість зберігатися у вигляді структурованих об'єктів файлів чи документів. Отже неструктуровані дані - дані, які не відповідають заздалегідь визначеній моделі даних, і, як правило, представлені у вигляді тексту з датами, цифрами, фактами, які розташовані в ньому в довільній формі[6]. Такі дані важко аналізувати, особливо з допомогою традиційних програм, призначених до роботи зі структурованими даними (анотованими або тими, що зберігаються у базах). Прикладом може слугувати неструктурований текст, книги, журнали, документи, метадані, аудіо, відео або фото, аналогові дані, повідомлення електронної пошти, вебсторінки, документи, створені за допомогою текстових процесорів.

Висновок

Сучасні інформаційні системи все більше мають справу з неструктурованою інформацією в умовах певної невизначеності. Складні бізнес процеси та зростаючі вимоги користувачів до систем обробки інформації вимагають високоефективних рішень. Це накладає обмеження на використанням та залучення сучасних підходів оброблення інформації. Інколи нема часу на системний аналіз та дослідження. Як результат з'являються системи адаптивного кейс менеджменту (Adaptive Case Management, ACM). Системи такого роду має на меті вирішення задач в умовах невизначеності та динамічної зміни. В ACM системах активно використовуються різноманітні мобільні пристрої. Гармонійна інтеграція та використання сучасних технологій є запорукою розвитку. Складність таких систем полягає в тому що захист інформації є пріоритетом та використання мобільних пристроїв ставить перед інженерами та розробниками нові складні технічні завдання.

Швидкій ріст технологій та використання мобільних простоїв в сучасному житті людини, функціональні можливості мобільних платформ вимагають певних заходів

безпеки у контексті зберігання даних. Обчислювальні потужності та надійний доступ до якісної швидкісної мережі призводить до того що частина приватної та критичної інформації потрапляє в цифровий світ на умовах неконтрольованого використання. Робота зловмисників стає більш складною та винахідливою. Користувач мобільних пристроїв має конкретні вимоги та побажання що спарюються на ергономіку та рівень інформаційної обізнаності. Слід зазначити що розвиток інформаційної галузі в цілому вимагає швидких, надійних та ефективних рішень що потрапляють не лише в економічну площину а й площину кібер безпеки.

Література

1. Adaptive Case Management, ACM; available at: *https www.it.ua/knowledge-base/technology-innovation/adaptive-case-management-acm* (accessed 5 December 2022).

2. Adaptive Case Management (ACM) (англ.); available at *https://web.archive.org/web/20180329082822/http://adaptive-case-management.com/* (accessed 5 December 2022).

3. Adaptive Case Management Global Excellence Awards (англ.); available at *http://adaptivecasemanagement.org/* (accessed 5 December 2022).

4. Android Marks Fourth Anniversary Since Launch with 75,0 % Market Share in Third Quarter, According to IDC; available at *https://web.archive.org/web/20121103041944/http://www.idc.com/getdoc.jsp?containerId=prUS23771812#.UOf0JG8z30Q/* : (accessed 5 December 2022).

5. Containerization is a winning strategy for smarter BYOD management. BetaNews (англ.). 20 квітня 2015. Архів оригіналу за 2 лютого 2022. Процитовано 2 лютого 2022.

6. Леонід Черняк. Аналітика неструктурованих даних . Відкриті системи. СУБД, 2012. № 06.

7. Unstructured data available at: *geeksforgeeks.org; https://www.geeksforgeeks.org/what-is-unstructured-data/* (accessed 5 December 2022).

References

1. Adaptive Case Management, ACM; available at: *https://www.it.ua/knowledge-base/technology-innovation/adaptive-case-management-acm* (accessed 5 December 2022).

2. Adaptive Case Management (ACM) (англ.); available at *https://web.archive.org/web/20180329082822/http://adaptive-case-management.com/* (accessed 5 December 2022).

3. Adaptive Case Management Global Excellence Awards (англ.); available at *http://adaptivecasemanagement.org/* (accessed 5 December 2022).

4. Android Marks Fourth Anniversary Since Launch with 75,0 % Market Share in Third Quarter, According to IDC; available at *https://web.archive.org/web/20121103041944/http://www.idc.com/getdoc.jsp?containerId=prUS23771812#.UOf0JG8z30Q/* : (accessed 5 December 2022).

5. Containerization is a winning strategy for smarter BYOD management. BetaNews (англ.). 20 квітня 2015. Архів оригіналу за 2 лютого 2022. Процитовано 2 лютого 2022.

6. Leonid Cherniak. Analityka nestrukturovanykh danykh Vidkryti systemy.[Analytics of unstructured data. Open systems]. SUBD, 2012. № 06.

7. Unstructured data available at: *geeksforgeeks.org; https://www.geeksforgeeks.org/what-is-unstructured-data/* (accessed 5 December 2022).

УДК 004.01,004.622, 004.912

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМИ СПОВІЩЕННЯ МОРЕПЛАВЦІВ ПРИ ВИЯВЛЕННІ НЕВІДОМИХ НЕБЕЗПЕК СХОЖИХ НА МОРСЬКІ МІНИ

DOI 10 36994 / 2788- 5518- 2022-02-04-19

Василенко А.О. *Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. vartudytu@gmail.com*

Павленко В. І. *, к.т.н., доц. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. pavlenko.v@i.ua*

Анотація: *У статті розглядається система для передачі даних NAVTEX в режимі вузькосмугового друкування (УБПЧ - NBDP - Narrow Band Direct Printing) та режимі телеграфії (F1B - телеграфія (TLX) з частотною модуляцією. Для роботи даної системи передбачено правову та технічну базу згідно Конвенції СОЛАС-74, з імплементацією кожної з країн підписантів, норм Конвенції до національного законодавства та технічних характеристик обладнання для передачі даних на морі.*

Розглядається розділення Світового океану на морські географічні райони в межах, яких навігаційні служби всіх країн світу, здійснюють свої обов'язки з забезпечення інформації з безпеки на морі для мореплавців. Одним з обов'язків є сповіщення мореплавців попередженнями, повідомленнями щодо ситуації на морі. У прибережних попередженнях поширюється інформація, яка необхідна для безпечного мореплавства в межах певного регіону. Зазвичай прибережні попередження надають інформацію, достатню для безпеки мореплавства далі за підхідний буй або лоцманську станцію, і не обмежуються інформацією щодо основних судноплавних шляхів.

Для передавання прибережних попереджень через NAVTEX, забезпечує передавання й автоматичне приймання інформації без залучення суднових фахівців. Відповідно до Регламенту радіозв'язку основною частотою, на якій передається цей вид інформації англійською мовою, є частота 518 кГц. Для передач NAVTEX національними мовами виділено частоту 490 кГц і додатково для тропічних районів - 4209,5 кГц. Навігаційні попередження кожного виду мають свою наскрізну нумерацію протягом усього календарного року, починаючи з номера 0001 на 00.00 годин Всесвітнього координованого часу по Гринвічу - (UTC) 01 січня.

Пропонується створити повідомлення відповідно до стандартів ухваленої Конвенції СОЛАС-74, щодо небезпеки у морі в межах певних координат (координати в форматі системи WGS 84). За прикладом, небезпеку становитиме об'єкт схожий на морську міну. В наведеному прикладі дані будуть наводитись зі скороченнями, як прийнято за стандартами при передачі подібних повідомлень, з метою зменшення об'єму найбільш необхідної інформації мореплавцям.

Ключові слова: *морська навігація, телеграфія, передача даних.*

PECULIARITIES OF USING THE MARINERS' WARNING SYSTEM WHEN DETECTING UNKNOWN HAZARDS SIMILAR TO SEA MINES

Artem Vasilenko . *Open International University of Human Development "Ukraine" , Kyiv, Ukraine. vartudytu@gmail.com*

Volodymyr Pavlenko *, Ph.D.,Ass. Prof. Open International University of Human Development "Ukraine. Kyiv, Ukraine. pavlenko.v@i.ua*

Abstract: *the article describes the system for data transmission NAVTEX with mode of narrow band printing (NBDP - Narrow Band Direct Printing) and telegraphy mode (F1B - Telegraphy (TLX) with frequency modulation. The system is operated by legal and technical basics which are provided in accordance with the SOLAS-74 Convention, an implementation of each of the signatory countries, norms of the Convention in the national legislation and technical characteristics of equipment for data transmission at sea.*

Under review, the World Ocean which is divided into maritime geographical areas within the navigation services of all countries of the world carry out their duties to provide maritime safety information to. One of the responsibilities is to notify mariners with warnings, messages about the situation at sea. Coastal warnings disseminate information that is necessary for safe navigation within a particular region. Usually coastal

warnings provide information sufficient for safe navigation beyond the approach buoy or pilot station and are not limited to information on the main shipping lanes.

Transmission of coastal warnings is done through NAVTEX, it provides the transmission and automatic reception of information without an involvement of shipboard specialists. According to the Radio Regulations, the main frequency on which this type of information is transmitted in English is 518 kHz. The frequency 490 kHz is allocated for NAVTEX transmissions in national languages and additionally for tropical areas - 4209.5 kHz. Each type of navigational alert has its own end-to-end numbering throughout the calendar year, starting with the number 0001 at 00.00 hours of Coordinated Universal Time (UTC) on January 01.

In result, it is proposed to create a message in accordance with the standards of the adopted SOLAS-74 Convention, regarding the danger at sea within certain coordinates (coordinates in the format of the WGS 84 system). For example, the danger will be an object similar to a sea mine. In this example, the data will be given with abbreviations, as is customary for the transmission of such messages, in order to reduce the amount of the most necessary information to mariners.

Key words: *maritime navigation, telegraphy, data transmission.*

Вступ

Для забезпечення безпеки у морях і океанах, в сучасному світі використовують доволі розвинені та поширені методи зв'язку. З 1 січня 1992 відповідно до прийнятої Конвенції СОЛАС-74 було розроблено методологію, систему поділу зон світового океану на регіони і передбачено технічні можливості для передачі наступних повідомлень мореплавцям:

1. Навігаційні попередження (COASTAL);
2. Метеорологічна інформація (WEATHER FORECAST);
3. Інформація з пошуку та рятувальні дії (спасіння);
4. Попередження про піратські напади.

З прийняттям Конвенції СОЛАС-74 усі країни також взяли на себе зобов'язання імплементувати в свої національні законодавства пункти, що стосуються технічного забезпечення та функціонування NAVTEX (NAVigational TEleX) з виділенням під роботу даної системи окремих смуг радіочастот і розділити світовий океан та моря на зони відповідальності NAVAREA - NAVAREA (Navigation Area) в межах, яких країни власники морських територій повинні надавати оперативну інформацію мореплавцям.

Виконання досліджень

Система NAVAREA (NAVAREA Navigation Area) – це морські географічні райони Всесвітньої служби навігаційних попереджень метою яких є забезпечення інформації з безпеки на морі. З метою уніфікації системи передачі навігаційної та метеорологічної інформації і з метою забезпечення безпеки мореплавства розроблено світову службу навігаційних попереджень, що забезпечує координацію передавання навігаційних попереджень та повідомлень по радіо всіма морськими країнами.[6] Передачу здійснюють по районам, які представляють собою зони Світового океану поділеного на 16 районів NAVAREA:

"NAVAREA I - Північна частина Атлантичного океану"

"NAVAREA II - Південна частина Атлантичного океану"

"NAVAREA III - Середземне море"

"NAVAREA IV - Східна частина Атлантичного океану (Східне узбережжя США і Канади)"

"NAVAREA V - Узбережжя Бразилії (Південна Америка)"

"NAVAREA VI - Прибережні райони Аргентини та Уругваю"

"NAVAREA VII - Район від Південної Африки до Антарктиди (Атлантичний та Індійський океани)"

"NAVAREA VIII - Прибережні райони Індії"

"NAVAREA IX - Район Перської та Аденської заток і Червоного моря"

"NAVAREA X - Прибережні райони Австралії"

"NAVAREA XI - Південна Азія"

"NAVAREA XII - Західна частина Тихого океану"

"NAVAREA XIII - Прибережні райони Росії"

"NAVAREA XIV - Прибережні райони Нової Зеландії та Південної частини Тихого океану"
"NAVAREA XV - Прибережні райони Чилі (Західна частина Тихого океану)"
"NAVAREA XVI - Узбережжя Перу" [3]

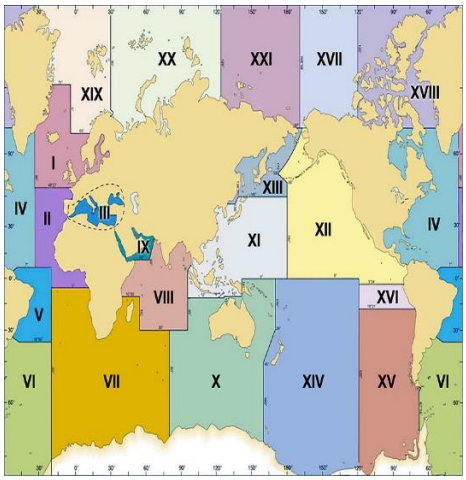


Рис. 1. Світові райони NAVAREA

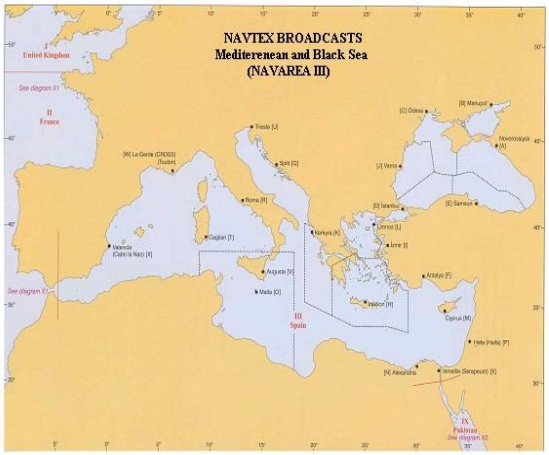


Рис. 2 Детальна мапа району NAVAREA III з Чорним та Середземноморським морями

Кожна з країн є відповідальною за безпеку проходження суден в межах своїх морських кордонів. Центри навігаційної інформації цих країн дають сповіщення стосовно забезпечення безпеки мореплавання. Крім того, є ще штаби кожного з районів NAVAREA, які додатково комунікують з усіма країнами, що входять в зазначені райони (їх називають районними координаторами NAVAREA). В сповіщеннях, які ще називають «повідомлення мореплавцям», повинна міститись інформація, що стосується пошкоджень небезпек, а також інформація, до якої можуть бути внесені зміни щодо запланованого маршруту, до такої інформації відносяться:

1. "несправність вогнів, туманних буїв і сигналів, що забезпечують плавання по основним судноплавними шляхами";
2. "наявність небезпечних затонулих суден на основних судноплавних шляхах в безпосередній близькості від них";
3. "встановлення нового важливого навігаційного обладнання або істотні зміни наявного, якщо таке встановлення або зміни можуть вплинути на безпеку плавання";
4. "наявність великих буксирних караванів в районах з туги плавання";
5. "дрейфують міни";
6. "райони пошуку-рятувальних робіт і райони, в яких проводяться заходи по боротьбі із забрудненням моря";
7. "наявність нововиявлених скелястих мілин, рифів і затонулих суден, які можуть становити небезпеку для мореплавства та, якщо є, їх огородження";
8. "несподівані зміни або тимчасова заборона плавання";
9. "робота з прокладання підводних кабелів або трубопроводів або інших підводних робіт, які можуть становити небезпеку мореплавства на судноплавних шляхах";
10. "значні порушення режиму роботи радіотехнічних засобів навігаційного обладнання";
11. "інформація, що стосується особливих дій, які можуть вплинути на безпеку мореплавання в деяких випадках в великих районах (навчання військово морських сил, ракетні стрільби і ін.)".

З першу наведена інформація оголошується відповідним районним координатором по можливості не пізніше ніж за 5 діб до початку своєї дії. Ці повідомлення повинні повторюватися до завершення їх дії в міру необхідності.

Розклади передач кожного району складаються так, щоб час передачі NAVAREA по даному району не збігався з часом подібних передач сусідніх районів, щоб не створювати радіоперешкод між іншими передачами від національних навігаційних відомств.

Якщо навігаційні попередження залишаються в силі після останньої передачі їх по радіо, то інформація що міститься в них, доводиться до відома мореплавців всього Світу.

Для того, щоб на судах не було повторного прийому одних і тих же попереджень і непотрібного очікування, берегові радіостанції передають свої NAVAREA почергово, переліком з кінця.

Передані по радіо NAVAREA повинні, як правило, містити інформацію тільки по своєму району. Передачі ведуться у встановлений час і повторюються по радіо відразу ж після початкової передачі, потім - у міру необхідності. NAVAREA, як правило, передаються від 2 до 6 разів на добу, повторюються по радіо від 30 до 45 діб після першого оголошення.

Бюлетені попереджень NAVAREA передаються періодично. Всі NAVAREA залишаються в силі до тих пір, поки вони не будуть скасовані районним координатором. В свою чергу, Кожен районний координатор повинен забезпечити інших районних координаторів або національні органи за їх запитами письмовими текстами попереджень NAVAREA, що мають термін дії більше 6 тижнів.

Друковані NAVAREA можуть видаватися портовими службами та адміністраціями, а де це можливо, їх включають в загальнодоступні друковані видання. У кожному районі ведеться своя порядкова нумерація переданих по радіо NAVAREA, починаючи з 1 січня кожного року. [5]

Система NAVTEX (NAVigational TEleX) - це міжнародна система для автоматизованого передавання навігаційної, метеорологічної, інформації з безпеки мореплавства, штормових попереджень та іншої термінової інформації в режимі вузькосмугового друку (ВБСЧ - NBDP - Narrow Band Direct Printing), режим (F1B - телеграфія (TLX), частотна модуляція (діапазон ПВ/КВ із ЦІМ + printer)). Повідомлення NAVTEX передаються береговими станціями, які перебувають у прибережній зоні, і радіус їхньої дії до 400 морських миль (близько 740 кілометрів).

Для служби NAVTEX спеціально виділено кілька частот у середньохвильовому діапазоні: 518 кГц (міжнародна), 490 кГц і 424 кГц (національні). Крім цього, для національних служб NAVTEX виділено частоти в короткохвильовому діапазоні: 4209.5 кГц. Тобто на частоті 518 кГц працюють берегові станції, що передають інформацію англійською мовою за всесвітнім розкладом, де для кожної берегової станції виділено спеціальний проміжок часу для передачі інформації.[2]

Розклад складається Всесвітньою Службою Навігаційних Попереджень. Для приймання повідомлень NAVTEX використовується спеціальний приймач, що складається з блоку приймача середньохвильового діапазону і друкувального пристрою. Згідно з вимогами GMDSS і SOLAS приймач NAVTEX встановлюють на містку або в штурманській рубці, він має бути постійно в робочому стані під час рейсу судна.

Передавальні станції NAVTEX географічно розташовані так, щоб під час їхньої роботи унеможливлювалися взаємні перешкоди. Щоб уникнути взаємних перешкод, усі берегові станції NAVTEX передають інформацію за розкладом, і кожна виходить в ефір не більше шести разів на добу.

Складання повідомлення для передачі пропонується для мореплавців згідно встановленої інструкції «По складанню й оформленню прибережних попереджень і доведенню їх до відома мореплавців» з розшифруванням тексту у повідомленні.

Рис. 3. Приймач NAVTEX з екраном. Furuno-nx-700b

Рис. 4 Приймач NAVTEX з лентою для друку повідомлень,. Furuno-nx-700a [4]

Розглянемо ситуацію, коли патрулюючи прикордонне судно виявило невідомий об’єкт, схожий на дрейфуючу міну у морських водах України. Про даний інцидент було повідомлено у навігаційний центр, а тепер з цього центру потрібно попередити усіх мореплавців про можливу небезпеку на морському шляху:

ЖИТТЄВО ВАЖЛИВО ***ПУНКТ ОДИН*** **НЕВІДОМИЙ ОБ'ЄКТ** **СХОЖИЙ НА МІНУ ДРЕЙФУЄ** 46-34.46N 031-30.41E **171215 UTC ЛЮТ 2022** **ДРЕЙФУЄ У НАПРЯМКУ 200 ГРАДУСІВ** ***ПУНКТ ДВА*** **ВІДМ ЦЬОГО** **201215 UTC ЛЮТ 2022**	VITAL ***PARA ONE*** **UNKNOWN OBJECT** **APPARENTLY MINE** 46-34.46N 031-30.41E **171215 UTC FEB 2022** **ADRIFT IN DIRECTION 200 DEGREES** ***PARA TWO*** **CANCEL THIS MSG ON** **201215 UTC FEB 2022**

Дане прибережне-навігаційне попередження буде поширене національною, та обов’язково англійською мовами, оскільки у морських водах можуть бути не українські судна, а і судна під іноземним прапором. [1]

Пункт «ЖИТТЄВО ВАЖЛИВО» вказує, що це важливе повідомлення, якщо при передачі ще додати до тексту * , то дане повідомлення також неможливо буде додати у виключення та проігнорувати приймачем. Повідомлення буде негайно передане по радіо.

Пункт «ПУНКТ ОДИН НЕВІДОМИЙ ОБ'ЄКТ СХОЖИЙ НА МІНУ ДРЕЙФУЄ» повідомляє про що йдеться у повідомленні. В нашому випадку виявлено об’єкт схожий на міну.

Пункт «46-34.46N 031-30.41E» вказує координати. В даному випадку в районі між Одесою та Очаковом.

Пункт «171215 UTC ЛЮТ 2022» вказує час за Гринвічем та дату коли було виявлено небезпечний об’єкт.

Пункт «ДРЕЙФУЄ У НАПРЯМКУ 200 ГРАДУСІВ» вказує напрямок руху на схід.

Пункт «*ПУНКТ ДВА* ВІДМ ЦЬОГО 201215 UTC ЛЮТ 2022» вказує час за Гринвічем та дату коли дане повідомлення припиняє свою дію.

Після припинення дії даного повідомлення, воно повинно бути опубліковано в публічному архіві на офіційних ресурсах розповсюдження інформації навігаційного центру. Повідомлення публікуються, як збірник текстових повідомлень в тому ж вигляді, як вони транслювалися під час передачі.

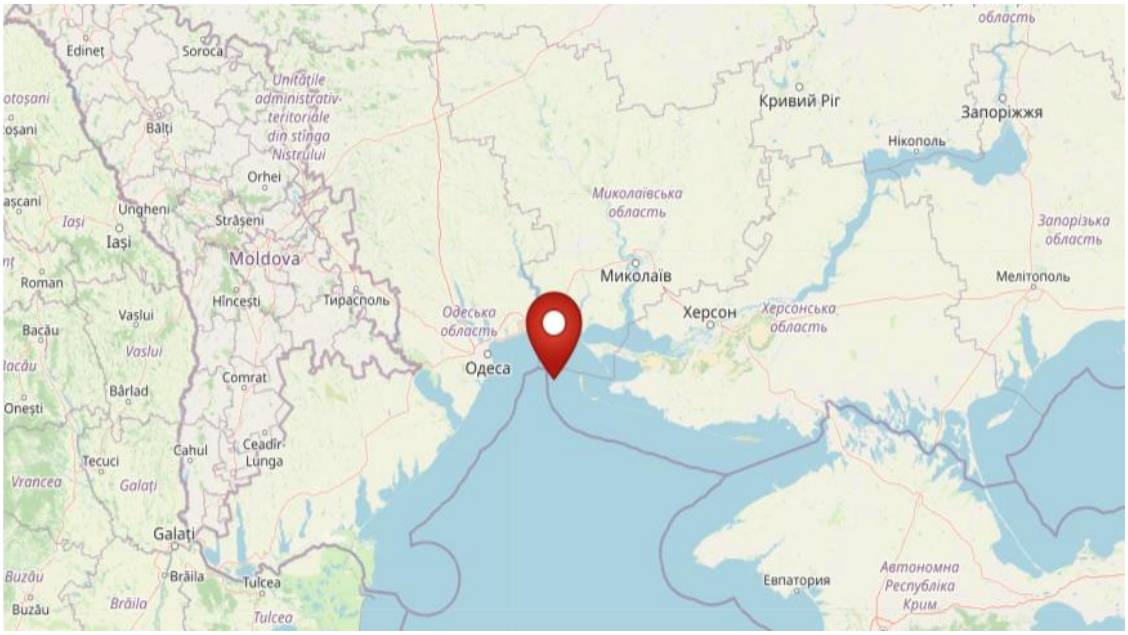


Рис. 5. Координати 46-34.46N 031-30.41E на мапі

Можливим вдосконаленням не тільки архіву а і можливостей системи загалом може стати графічна оболонка з можливим відображанням даних по оновленню ситуації на морі. Підчас роботи навігаційного центру у надзвичайних ситуацій кожна хвилина граю свою вагому роль для забезпечення безпеки суден під час навчальних стрільб або під час пошуко-рятувальних робіт. Дане вдосконалення дозволило б зменшити час роботи і відійти від використання паперових мап у навігаційних центрах. Для публічних користувачів було б набагато зручніше орієнтуватися за графічною мапою ніж за координатами у системі WGS 84.

Висновки

NAVTEX (NAVigational TEleX) та NAVAREA (Navigation Area) зарекомендували себе, як надійну систему регулярного сповіщення мореплавців. Повідомлення, як розглядалось у статті, буде передане миттєво при наступній трансляції. Так буде попереджено усі судна, які проходять біля зазначених координат і буде врятовано багато життів.

Серед недоліків слід відмітити, що при транслюванні повідомлення згідно розкладу на виділених частотах 518 кГц, 490 кГц, 424 кГц, 4209.5 кГц, якщо відбувається паралельна трансляція, це прямо впливає на якість повідомлень через накладання одного сигналу на інший в межах однієї смуги радіочастот. Даний технічний недолік усувається тільки організаційними заходами, районний координатор кожної із зон NAVAREA формує розклад кожної національної навігаційної служби для подальших трансляцій у відведений час.

Інший недолік, це відсутність інструментів для графічної візуалізації, що вирішується технічними можливостями сьогодення. Графічна оболонка була б актуальної, як і для працівників та службовців навігаційних центрів, так і для користувачів, яким потрібно візуально проста інформації щодо ситуації на морі.

Література

1. Вісник Держгідрографії, №4, Держгідрографія, Київ ,2010. с.12.
2. Міжнародна Гідрографічна Організація. Посібник з інформації з безпеки на морі (MSI). Монако ,2016 . с.11.
3. Підручник NAVAREA – NAVTEX, в редакції від 2021, розділ III.URL:http://ni.biz.ua/14/14_2/14_26062_III-preduprezhdeniya-navarea.html

4. Міжнародна конвенція з охорони людського життя на морі СОЛАС-74, ІМО, з поправками від 2004, розділи IV та V.
5. Офіційна документація до приймачів Furuno NAVTEX, Нісіномія, Японія, 2006.с.16.
6. Корякін А. Інструкція по складанню й оформленню прибережних попереджень і доведенню їх до відома мореплавців : Держгідрографія, Київ 2003. 20-21 с.

References

1. Visnyk Derzhhidrohrafii [Bulletin of the State Hydrography].№4, Derzhhidrohrafiia, Kyiv ,2010. s.12.
2. Mizhnarodna Hidrohrafichna Orhanizatsiia. Posibnyk z informatsii z bezpeky na mori [.nternational Hydrographic Organization, Manual on maritime safety information (MSI)], Monaco 2016. p.11
3. Pidruchnyk NAVAREA – NAVTE [Digital source], NAVAREA - NAVTEX , Manual, 2021, chapter III..URL: http://ni.biz.ua/14/14_2/14_26062_III-preduprezhdeniya-navarea.html
4. Mizhnarodna konventsiia z okhorony liudskoho zhyttia na mori SOLAS-74_.[International Convention on the Protection of Human Life at Sea SOLAS-74], IMO, z popravkamy vid 2004, rozdily IV ta V.
5. Ofitsiina dokumentatsiia do pryimachiv Furuno NAVTEX.[International Convention for the Safety of Life at Sea] SOLAS-74, IMO, amended in 2004, chapters IV and V.
6. Koryakin A. Instruktsiia po skladanniu y oformlenniu pryberezhnykh poperedzhen i dovedenniu yikh do vidoma moreplavtsiv.[Instruction for compiling and issuing Coastal warnings and bringing them to the attention of mariners]. Derzhhidrohrafiya, Kyiv, 2003.pp. 20-21 .

УДК. 004.658.2

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФРАСТРУКТУРИ БАЗ ДАНИХ ДЛЯ ФІНАНСОВОГО СЕКТОРУ

DOI 10 36994 / 2788- 5518- 2022-02-04-20

Рожков С.М. *Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. serj.rozhkov@gmail.com*

Анотація: *Метою цієї статті є дослідити та спрогнозувати етапи та шляхи розвитку інфраструктури для баз даних фінансових установ, що пов'язані із індустріальними регуляціями. Розглянуто основні тенденції в IT в цілому та у вибраному домені, наведені порівняльні розрахунки для безсерверних хмарних сервісів та самоінстальованих баз даних.*

Ключові слова: *бази даних, AWS, публічна хмара, безсерверні технології, RDS, EC2, фінансовий сектор.*

PROSPECTS OF THE INFRASTRUCTURE DEVELOPMENT FOR FINTECH COMPANY'S DATABASES

Sergii Rozhkov. *Open International University of Human Development "Ukraine",Kyiv, Ukraine. serj.rozhkov@gmail.com*

Abstract: *Technologies used in the development of applications are changing rapidly On the other hand, one of the main parts of the backend is a database which does not undergo fundamental changes so often. The purpose of this work is to investigate and, if possible, to predict ways of fintech companies' infrastructural solutions for the nearest future.*

One of the biggest users of relational databases is the financial sector. In order to predict something, one must first determine the current state of database infra. By 2020, almost 75 percent of the infrastructure was located on real servers in rackspaces. Despite all this, most fintech companies plan to move to public clouds in the future as it provides

many advantages for their business. Even 5-7 years ago, it was not possible to talk about the fact that highly loaded databases of serious financial companies could be deployed in the public cloud, since public clouds could not provide the necessary performance, primarily in the speed of working with the volumes[1][4]. But progress in hypervisor technologies has led to the fact that almost any database can be migrated or deployed in the cloud. Therefore, it is safe to say that the future deployment of database infrastructure are public or private clouds.

But the use of serverless technologies (for example, RDS in AWS) will still not gain such a large popularity. Since so far self-installed databases are cheaper not only in terms of hardware, but also in terms of licenses for paid versions of databases. In addition, self-installed versions provide greater flexibility and maneuverability in solving emerging issues during operation, for example, to work with a disk, you can use software RAID for disks of different types, distribute the load on different partitions (for example, database files on one partition, log files on another partition)[1] or use optimization due to the file system itself and its additional options, use combinations of instances with ephemeral storage and orchestrators and configuration management systems for read-only replications.

Key words: *databases, AWS, public cloud, serverless services, RDS, EC2, fintech.*

Вступ.

В сучасному бізнесі існує велика конкуренція яка і є рушієм прогресу, а для кінцевих користувачів виражена у тому що сервіси постійно покращуються, не є виключенням і фінансовий сектор де, наприклад, вже важко знайти людино у якої буде менше двох мобільних банкінгів на смартфоні. Тому, як ми бачимо, навіть тут, де кожна дія обмежена індустріальними та урядовими регуляціями треба орієнтуватися на високопродуктивні фреймворки, безсерверні та хмарні технології – щоб бути швидшим, кращим і давати те чого немає у конкурентів.

Технології що використовуються у розробці застосунків змінюються швидко, але, не зважаючи на це, однією із основних частин бекенду є бази даних де корінні зміни відбуваються не так часто, тому в даній статті основна увага буде приділена саме базам, так як окрім того шо це є важливим елементом він, як правило, є ще і найдорожчою частиною архітектурного рішення.

Як видно із рис.1. одним із найбільших користувачів реляційних баз даних є саме фінансовий сектор.

Виконання досліджень

Для того щоб щось прогнозувати треба спочатку визначитися із поточним станом речей. На 2020 рік майже 75 відсотків інфраструктури знаходилися саме на «залізних» серверах(див рис.2.)

Але якщо подивитися на топових користувачів саме хмарних сервісів (рис.3.)[7] то можна побачити що саме фінансовий сектор є одним із лідерів по інтеграції своїх сервісів, хоча захист облікових даних – одна з найбільших проблем, пов'язаних із розташуванням даних у хмарі. Візьмемо, наприклад, AWS (Amazon Web Services). Оскільки з вашого кореневого облікового запису здійснюється керування пов'язаними ресурсами та сервісами AWS, потрібно надати повний доступ до всіх даних, включаючи ті, на які поширюються права адміністратора.

Рис.1. Статистика використання баз даних за індустрією.

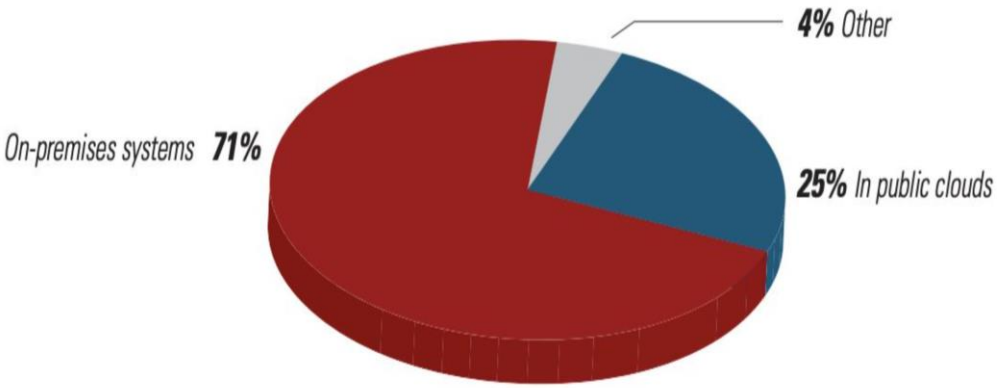


Рис.2. Розміщення інфраструктури оператора.

Рис.3. Лідери використання хмарних сервісів.

Незважаючи на все це, більшість фінтек компаній планує і надалі переїздити у публічні хмари(рис.4.) так як це надає безліч переваг[3]:

- більша гнучкість масштабування;
- менший кошторис;
- не потрібно витрачати час на підтримку серверної інфраструктури;
- швидший шлях сетапу від розробки до продакшену;
- менший рівень кваліфікації персоналу;
- більший вибір СУБД;
- інтеграція із іншими хмарними сервісами;
- швидкі бекапи;
- можливість переносити пікове навантаження із нарощуванням потужності;
- краще балансування навантаження.

Згідно із рис.5 основні зусилля європейських компаній витрачаються саме на міграцію у хмари і, як бачимо, далі на оптимізацію коштів, що і не дивно, так як тарифікація сервісів є багатовекторною і складною. Це навіть породило компанії які просто прораховують вартість майбутньої конфігурації інфраструктури, а потім контролюють рахунок і надають свої рекомендації щодо його оптимізації.

	Past 12 months	Next 12 months
Decrease	2%	2%
No change	32%	18%
Increase 1–5%	18%	15%
Increase 6–10%	16%	17%
Increase 11–25%	13%	17%
Increase 26–50%	9%	11%
Increase by more than 50%	4%	10%
Total Increase	**26%**	**38%**
Don't know/unsure	7%	9%

Рис.4. Найближчі плани стосовно міграції баз даних у хмарні сервіси.

Рис.5. На які роботи у хмарі витрачають ресурси європейські компанії

Із наведеної вище статистики випливає лише один висновок – надалі більшість компанії будуть переносити свої як звичайні сервіси і застосунки там і бази даних саме у публічні хмари.

Розглянемо ефективність використання коштів, так як перш за все мета бізнесу -це більше заробляти та менше витрачати. А далі відштовхуватися від результатів. Публічна хмара, мабуть, найбільш економне рішення, особливо якщо ви працюєте з SaaS-додатком зі зростаючими вимогами до інфраструктури. Приватна хмара, навпаки, буде найкращим варіантом, якщо контроль та безпека для вас найважливіша. Так як найпопулярнішим публічним хмарним сервісом є AWS далі будемо розглядати само його(рис.6.).

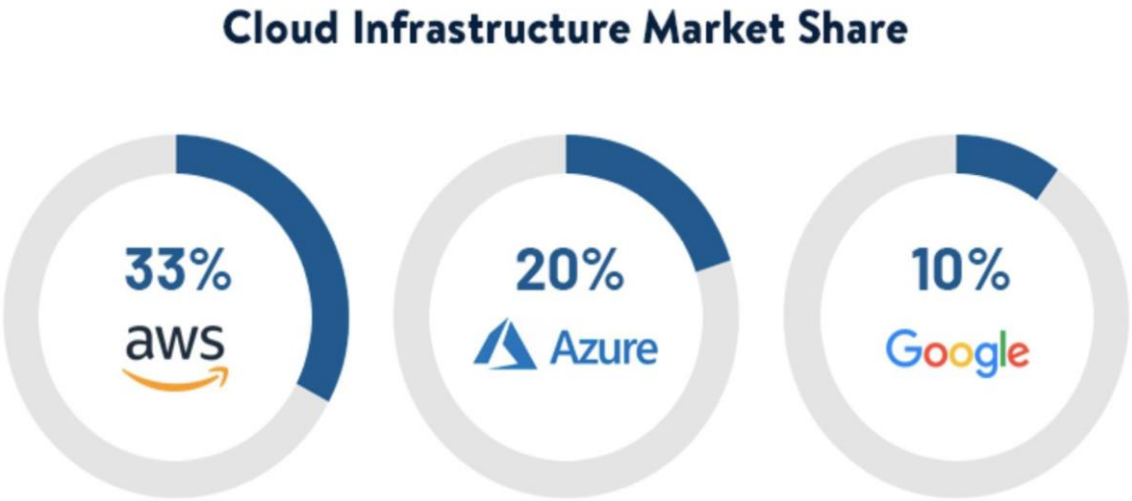


Рис.6. Статистика використання хмарних сервісів.

Далі постає питання – чи треба використовувати хмарні сервіси баз даних чи все ж використовувати самоінстальовану базу даних.

Розглянемо AWS RDS (Relational Database Service) – це база даних як сервіс. Вам надають доступ до бази даних без необхідності її адмініструвати, а всі турботи щодо підтримки резервного копіювання, налаштування реплікації та забезпечення високої доступності бере на себе постачальник послуги (тобто AWS)[5].

Простіше кажучи ви отримуєте один або кілька екземплярів БД, з якими можна одразу працювати – писати чи читати дані. При цьому немає необхідності самостійно розбиратися з встановленням та початковою конфігурацією самої БД. Але, насправді, є нюанси. Обмеження RDS можна загалом сформулювати так[2]:

- оскільки весь процес адміністрування бере на себе провайдер, ви як користувач отримуєте обмежену можливість конфігурування БД, що іноді буває критично, тому що при цьому відсутня можливість при необхідності зробити тонке налаштування;
- із точки зору безпеки ви навіть не маєте користувача із повним набором адміністративних привілеїв;
- якщо хтось робить за вас всю «брудну» роботу, то за це доведеться заплатити, а у випадку RDS рахунок буває чималим.

Зробимо невеличкий примірний підрахунок-порівняння між RDS та самоінстальованою базою на EC2. Для прикладу візьмемо базу середнього розміру із параметрами 32 CPU 128 RAM. Для простоти прикладу візьмемо звичайний SSD диск на 1Tb.

Для RDS:

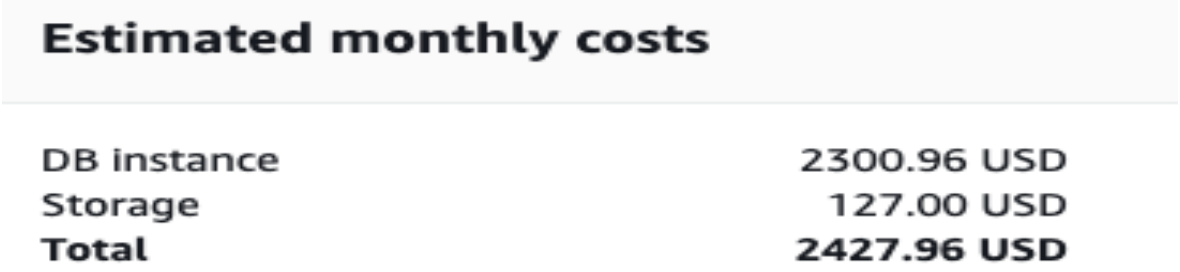


Рис.7. Розрахунок вартості інстансу RDS із майстер нодою

Якщо додати ноду для репліки:

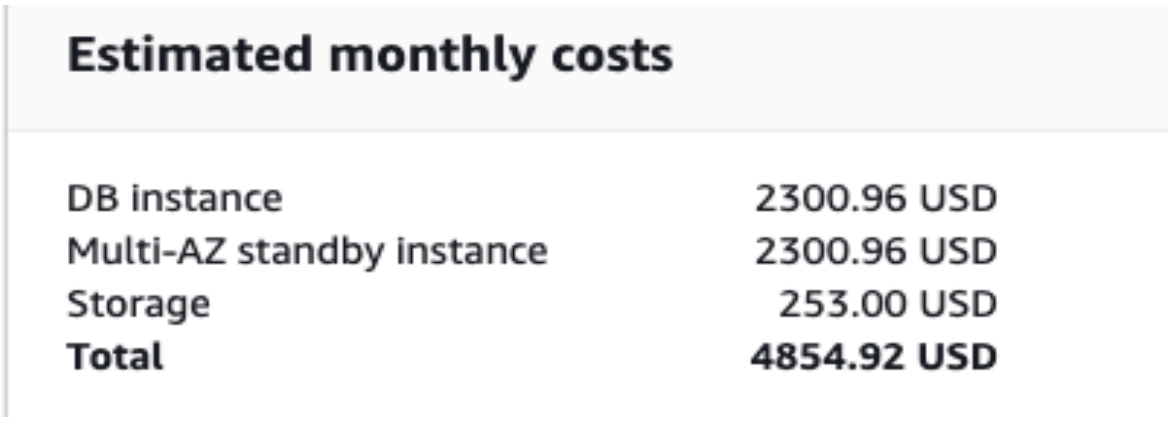


Рис.8. Розрахунок вартості інстансу RDS із майстер нодою та реплікою

Приклад для бази на EC2:

Estimated monthly costs

	instance type	hour	day	month	storage per Gb	1 Tb	Total
master	m6i.8xlarge	1,712	41,088	1232,64	0,11	110	**1342,64**
					Total		**1342,64**

Рис.9. Розрахунок вартості інстансу EC2 із майстер нодою

Із реплікою:

Estimated monthly costs

	instance type	hour	day	month	storage per Gb	1 Tb	Total
master	m6i.8xlarge	1,712	41,088	1232,64	0,11	110	**1342,64**
replica	m6i.8xlarge	1,712	41,088	1232,64	0,11	110	**1342,64**
						Total	**2685,28**

Рис.10. Розрахунок вартості інстансу EC2 із майстер нодою та реплікою

Як випливає із розрахунків – самостійно інстальована база даних в два рази дешевше, тобто, якщо ми говоримо про кластерну архітектуру для високонавантажених баз даних, різниця може сягати десятків тисяч доларів на місяць.

Також можна розглянути ліцензовані бази даних і порівняти їх ціни, візьмемо до прикладу дуже популярний Microsoft SQL Server:

- RDS RI 32 cores price - 178116$/рік
- Marketplace IAM 32 cores price - 137777$/рік + 15894$/рік за EC2 ісntанс
- Own License 32 cores - 95632$/рік + 15894$/рік за EC2 ісntанс

Це означає що із точки зору бізнесу повністю нівелюється головна перевага RDS – те що не треба мати окремого спеціаліста із баз даних, тому що для великих об’ємів вигідніше найняти команду DBA.

Часто буває, коли проект тільки починається, то вигідніше взяти RDS. Але в міру зростання та розвитку самого проекту зростає, як правило, і база даних, а значить і вартість за кожен екземпляр RDS. У якийсь момент приходить розуміння, що вигідніше мати self-hosted-рішення, навіть з урахуванням витрат на його розгортання та підтримку часу і ресурсів.

Висновок

Ще 5-7 років тому годі було говорити про те щоб високонавантажені бази даних серйозних фінансових установ могли бути розгорнуті у хмарі, так як публічні хмари не могли надати необхідну продуктивність насамперед у швидкості роботи із диском[1][4]. Але прогрес у технологіях роботи гіпервізора призвів до того що вже майже будь-яку базу можна мігрувати або розгорнути у хмарі. Тому можна впевнено говорити що майбутнє розгортання інфраструктури баз даних – це публічні або приватні хмари.

А ось використання безсерверних технологій(наприклад RDS у AWS) все ж не набуде такого великого масштабу. Так як поки що самоінстальовані бази даних окрім того що є дешевшими не тільки у плані заліза, а і у плані ліцензій на платні версії баз даних. Окрім того, самоінстальовані версії надають більшу гнучкість та маневреність по вирішенню виникаючих питань по мірі експлуатації, наприклад, для роботи із диском можна використовувати програмні RAID для дисків різних типів, розносити навантаження на різні розділи(наприклад на один розділ файли бази, на інший розділ файли журналів)[1] або ж використовувати оптимізацію за рахунок самої файлової системи та її додаткових опцій, використовувати комбінації із інстансів із ефемерним сторaджем та оркестраторів і систем управління конфігураціями для реплікацій що використовуються лише для читання.

References

1. Vinicius M. Grippa, Sergey Kuzmichev «Learning MySQL: Get a Handle on Your Data»
2. Hans-Jurgen Scholing «Mastering PostgreSQL 13: Build, administer, and maintain database applications efficiently with PostgreSQL 13», 4th Edition.
3. Brendan Gregg's "Systems Performance: Enterprise and the Cloud", 2nd Edition.
4. M. Ma, Z. Yin, "Diagnosing root causes of intermittent slow queries in cloud databases".
5. Shared Responsibility Model aws.amazon.com/ru/compliance/shared-responsibility-model.
6. Database in a cloud survey https://d1.awsstatic.com/whitepapers/RDS/IOUG-AWS-Databases-in-the-Cloud-Final-Report.pdf
7. Cloud cumputing statistic https://99firms.com/blog/cloud-computing-statistics/

УДК 004.622, 004.623, 004.632.4

СТІЙКІСТЬ ТА ЕФЕКТИВНІСТЬ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЩО ВИКОРИСТОВУЮТЬСЯ У МОБІЛЬНИХ ПРИСТРОЯХ

DOI 10 36994 / 2788- 5518- 2022-02-04-21

Середа А.В. *Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. andrew.sereda@gmail.com*

Даценко І.П. *к.т.н. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. docik_ivan@ukr.net*

Павленко В.І*. к.ф.-м.н. , доц. Відкритий міжнародний університет розвитку людини «Україна». Київ, Україна. pavlenko.v@i.ua*

Самарай В.П., *к.т.н., доц. Відкритий міжнародний університет розвитку людини, Київ, «Україна», Україна. samaraj@ukr.net*

Анотація: *у статті розглядаються новітні типи криптографічних алгоритмів у різних мобільних операційних системах(IOS, Android). Пропонується дослідити різні методи для оцінки стійкості та ефективності представлених алгоритмів. Криптоаналіз математичних моделей та фізичних приладів для захисту конфіденційної чи чутливої інформації.*

Ключові слова: *мобільні пристрої, криптографія, захист, безпека, стійкість, криптоаналіз, кібербезпека.*

STABILITY AND EFFICIENCY OF CRYPTOGRAPHIC ALGORITHMS USED IN MOBILE DEVICES

Andrey Sereda. *Open International University of Human Development “Ukraine”, Kyiv, Ukraine. andrew.sereda@gmail.com.*

Ivan Datsenko, *Ph.D. Open International University of Human Development “Ukraine”, Kyiv, Ukraine. docik_ivan@ukr.net.*

Volodymyr Pavlenko, *Ph.D., Ass Prof. Open International University of Human Development “Ukraine”, Kyiv, Ukraine. pavlenko.v@i.ua.*

Valerii Samarai, *Ph.D.,Ass Prof. pen Internationfl University of Human Development “Ukraine”, Kyiv, Ukraine. samaraj@ukr.net*

Abstrfct*: the article examines the latest types of cryptographic algorithms in various mobile operating systems (IOS, Android). Research describes how different operating systems protect user data; what vulnerabilities exist for now. Determine what is sensitive information for the user that should be carefully secured. Recommendations how to protect and increase security for mobile devices that are everywhere solving different tasks including digital actives. A lot of attention is paid to different technologies of protection, general principles of security of confidential data. Exploring existing levels of abstraction for design and analysis the stability or efficiency for cryptographic systems. Give a try to compare different environments with opposite ideology but one roots. Partial or complete breakdown, prompt response to vulnerability. The problem of disk space encryption and the choice of appropriate cryptographic algorithms by one or another platform are considered. It is proposed to investigate various methods for evaluating the stability and efficiency of the presented algorithms. Cryptanalysis of mathematical models and physical devices to protect confidential or sensitive information. An overview of end-to-end encryption and why it is important. Thoughts on further research on finding a universal method for checking the stability and efficiency, time or labor costs for the possibility of interfering with the security of the device under the condition of active floating or with the help of a hardware and software product are presented. At the end, conclusions and suggestions for improving the efficiency of the security system on any mobile device under the guidance of the operating system are presented. Everything invented by man or nature is subject to study and research in the possibility of obtaining benefits for humanity.*

Вступ

Однією із найважливіших характеристик криптографічного захисту інформації (КЗІ) вважається стійкість алгоритму до криптоаналізу. Тобто стійким вважається алгоритм, який для успішної атаки вимагає від противника недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень чи ж такого часу розкриття, що по його закінченню захищена інформація буде вже не актуальна, і т. д. У більшості випадків крипостійкість не можна математично довести, можна тільки довести уразливість криптографічного алгоритму[1].

Відомо [2], що існує декілька рівнів абстракції при проектуванні та аналізі стійкості криптографічних систем: абстрактна математична модель криптографічного перетворення (алгебраїчні та ймовірнісні моделі шифру), модель засобу криптографічного захисту інформації та криптосистеми реалізованій на конкретній програмно-апаратної платформі. Перші моделі переважно аналізуються методами класичного криптоаналізу, останні – криптоаналізу з використанням інформації з побічних каналів (англ. - side-channel cryptanalysis). Таким чином, у криптоаналізі побічними каналами досліджується вплив непрямої інформації, отриманої під час роботи криптосистеми, на ослаблення стійкості до часткового або повному зламу[2]. Очевидно, що методи криптоаналізу по побічним каналам залежить від архітектури та особливостей реалізації обчислювальної системи, у межах якої реалізовано засіб КЗІ.

На даний момент світовий ринок операційних систем для мобільних пристроїв з великим відривом очолюють двоє лідерів: Google Android та Apple iOS (**Рис. 1**)**.** У процесі еволюції обидві платформи сформували підходи до організації безпеки даних користувача. Кожна має свої переваги та недоліки. Закрите середовище розробки iOS та оперативне реагування на вразливість створюють довіру до Apple. Але досі Apple повністю не захищає користувачів від зламу та компрометації даних різними каналами.

Google за останні кілька років значно підвищила безпеку ОС Android за рахунок використання криптографічної функціональності. Але фахівці з кіберкриміналістики все ще можуть обійти захисні механізми Android та отримати доступ до даних.

Розглянемо детальніше кожну з операційних систем, розберемо методи захисту, позначимо сильні та слабкі сторони безпеки. У результаті сформуємо рекомендації як для користувачів, так і для розробників з обох платформ.

Виконання досліджень

Майже всі дані користувача мобільних пристроїв є конфіденційними: електронна пошта, повідомлення, біометрична інформація, фото- і відеоконтент, документи, місце розташування, паролі, історія роботи у браузері та багато іншого. Які саме дані найбільш конфіденційні і які техніка захисту використовуються зараз? Також розглянемо загальну модель загроз.

Можна виділити декілька ключових технік контролю доступу до даних:

- *Безпека та ізоляція ПО.* Сучасні операційні системи мобільних пристроїв чітко розмежовують доступ додатків і доступ користувача. Наприклад, сумнівні додатки не можуть отримати доступ до даних, на які не мають відповідних прав, дозволів. Для запуску довільного коду на пристрої необхідно виконати обхід встановленого обмеження: «джейлбрейк» для iOS або отримати рут-доступ для Android.
- *Доступ за допомогою кодів та біометрії.* Контроль доступу до інтерфейсуОС здійснюється переважно через пароль довільної сили, найчастіше він цифровий. Можна активувати паттерн (графічний ключ — послідовність) на екрані блокування. Все частіше застосовується біометричний доступ : через розпізнавання рис обличчя або відбиток пальця.

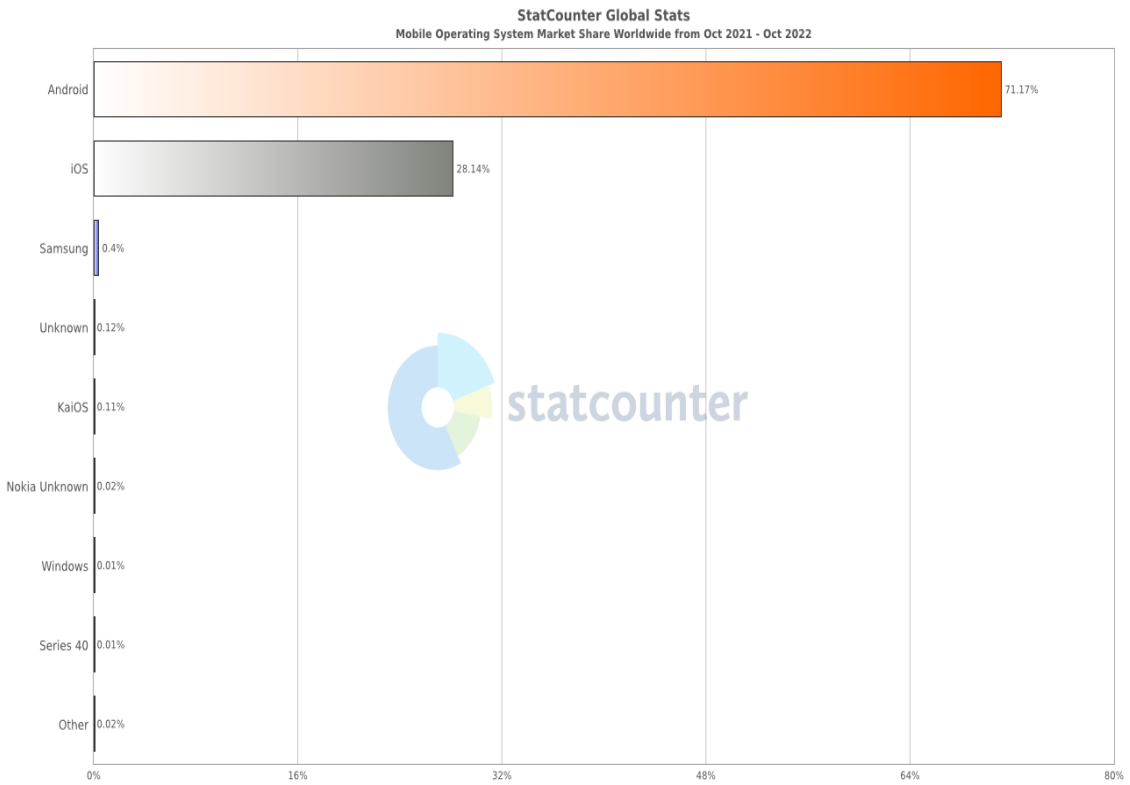


Рис. 1. Частка мобільних платформ у світі згідно statcounter.com

- *Шифрування файлів та дисків.* В разі обходу зловмисником програмних методів захисту він зіткнеться з зашифрованими даними. Це можуть бути, як окремі файли, так і розділи диска. Шифрування даних, як правило, організоване асиметрично: в обладнання вбудована одна частина ключа, а інша – генерується на основі вибраного користувачем паролю.
- *Безпечне апаратне забезпечення пристроїв.* Останнім часом виробники впроваджують співпроцесори безпеки та їх віртуалізовані аналоги. Це захищає від програмних атак і атак на обладнання пристрою, підсилюючи механізми шифрування конфіденційних даних, зокрема біометричних шаблонів.
- *Безпечне резервне копіювання та робота з хмаровими системами.* Зовсім недавно постачальники послуг почали пропонувати безпечну модель хмарного зберігання резервних копій даних з пристроїв. Сучасна система зашифрованого резервного копіювання унеможливлює прямий доступ хмарового провайдера, зловмисників чи правоохоронних органів до даних користувача

Модель загроз: Сучасні мобільні пристрої досить добре захищені від традиційних дистанційних атак. Але прямий фізичний доступ до пристрою (або його компонентів) протягом тривалого часу, значно спрощує роботу шахраїв або фахівців з кібербезпеки, що підвищує ризик зчитування інформації.

Прямий доступ може здійснюватися незаконно, (крадіжка, обман), або працівниками органів юстиції, кіберполіції законно, котрі виконують законодавчі приписи, що передбачають розсекречування паролей. Слід бути дуже обережним, оскільки не виключене використання державними чиновниками своєї службової компетентності та невігластва користувача. Це нашкодить в подальшому хорошій репутації пристрою. Треба завчасно перевіряти особисті документи та дозволи, бо шахраї часто користуються соціальною довірою, видають себе за співробітників правоохоронних, державних установ, і обізнані в інженерних техніках, легко проникають в бази мобільних пристроїв. Таке проникнення через застосування поля кіберкриміналістики допоможе не тільки скопіювати необхідну інформацію, але й мати токени доступу до безпечних хмарних сховищ, із пам'яті. Інформативні файли з мобільних пристроїв і

хмарних сховищ завжди містять в собі особисті дані, заволодіння якими становитиме загрозу конфіденційності користувачів.

Конфіденційність даних мобільних пристроїв.

Полюючи на злочинця**,** фахівці з кіберполіції дістають найбільш важливі категорії закритої інформації, яка допоможе розкрити злочин. Приміром за основу візьмемо:

- IMEI, MEID / ESN та інші показники абонента мобільного зв'язку;
- всі вихідні і вхідні дзвінки, залишені в журналах;
- списки контактів, календарні дати, нагадування і т. п.;
- відео та аудіо матеріали, файли з документами;
- різні види повідомлень (миттєві, MMS.SMS);
- адреса і вміст електронної скриньки;
- історія та закладки в браузері;
- координати місця знаходження та пересування;
- діяльність в соціальних мережах;
- SIM / UICC, провайдер, IMSI, MSISDN та інше.

Даний перелік не обов'язково має незаперечний характер. Частина відомостей може мати тимчасову актуальність. Але треба пам'ятати, що тісні мережеві зв'язки з родичами, колегами, друзями (особисті листування, розмови, коментарі) містять приватну інформацію та під час розголосу загрожують безпеці великої групи людей.

Компанія Apple, операційна система iOS.

Кількість працюючих гаджеті у всьому світі за підрахунками корпорації Apple в 2022 році перевищила 1, 5 млрд. одиниць. Це майже 46 % мобільних телефонів в США та інших країнах, що знаходяться під контролем операційної системи iOS. Постійне зростання кількості новинок Apple на руках у світової спільноти приваблює, як шахраїв, так і багхантерів (фахівців, що шукають проблемні місця, недоліки в програмах), які співпрацюють з корпорацією. На оплату послуг з тестування щорічно витрачається понад 2 млн доларів США.

Захист даних користувача iOS на сьогоднішній день

Основні елементи захисту формуються на тісній взаємодії Ключові елементи захисту сформовані за допомогою взаємозв'язку пристрою з хмарними технологіями.

Автентифікація

Користувачі фізично взаємодіють з пристроями через: біометричну аутентифікацію або код, що складається з літер та цифр. Переважно це пароль із шести символів, активований по замовчуванню. Рекомендується застосування довгих паролів, що складаються з цілих фраз (комбінацій слів, літер). Apple не радить повністю вимикати аутентифікацію, хоча така можливість існує. Кількаразові спроби набору паролю блокуються. Повторно ввести код дозволяється тільки через певний час. Вищий рівень захисту надають TouchID (датчик відбитку пальця) і FaceID (ідентифікація рис обличчя з допомогою камери).

Підписи кодів програм

Код, що виконується на iOS , простіше всього, обмежити з допомогою цифрового підпису, вбудованого на нижчому рівні (Boot ROM). В момент, коли підпис проходить перевірку, відбувається безпечна загрузка, яка гарантує тривалий захист від ініціалізації підозрілого коду) і за рахунок підпису додатка, яка складається із частини, контрольованої Apple і сертифікату з відкритим ключем для масштабування системи. Існують також «сертифікати підпису установи», призначені для спеціалізованого запуску додатків на iOS.

Пісочниця та аналіз коду

Убезпечити користувацькі дані і API від проникнення в систему підозрілих додатків допомагає запровадження обмеженого доступу до простору пам'яті, файлів через встановлення ізольованого

середовища, так званої пісочниці. При підписанні маніфесту спеціально вказуються ресурси і служби широкого доступу. До них належить геолокація. Додатки із App Store підлягають автоматичній та ручній перевірці коду. Хоча навіть найстрогіші обмеження не дають стовідсоткової гарантії перепони проникненню чужих небажаних додатків. Вони можуть пройти перевірку і порушити винятковість прав користувача.

Шифрування

В Apple діє також надійна система шифрування даних пристрою Data Protection. Це на випадок коли шахраям якимось чином все ж вдасться обійти попередні захисні механізми, приміром, через логічні прорахунки чи недоліки обладнання. Використовуються криптографічні стандарти AES, ECDH over Curve25519 та інше, те що схвалене NIST(Національним інститутом стандартів і технологій) США. Всі дані прикріплені до пристрою і їх контролює сам користувач. Тільки йому відомий ключ шифрування — унікальна апаратна секретна комбінація UID (криптоключ) і пароль. Якщо пристрій перезапускається, то ключ шифрування треба встановлювати заново, тобто ввести раніше встановлений пароль і розблокувати ключі з допомогою біометрії. Заважає обійти шифрування метод обмеження пропозицій із збільшенням інтервалів часу та функцією отримання ключа на основі паролю. Apple застосовує такі «класів захисту» (Class key) шифрування на вибір розробників:

- Повний захист (CP) —прилади ключі шифрування видаляються через 10 секунд після блокування.
- Захищено тільки, коли закрито (PUO) — в пам’яті залишається відкритий ключ передачі зашифрованих файлів, коли пристрій заблокований. Повний захист включається (CP) після створення файлу, в момент його закриття.
- Захищено до першого розпізнавання користувача — початкового розблокування (AFU). Коли вводиться перший раз пароль, то ключі шифрування розблоковуються і залишаються в пам’яті пристрою навіть під час блокування.
- Захист відсутній (NP) —пристрій включений, шифрування здійснено тільки апаратними ключами UID і до них постійно є доступ в пам’яті, коли пристрій працює.

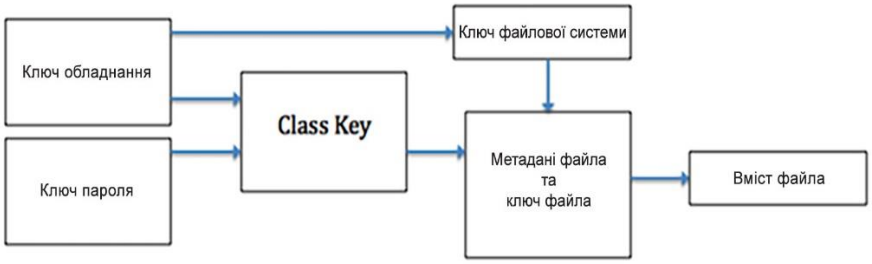


Рис. 2. Схема ієрархії ключів iOS Data Protection

Keychain

Це — захищене апаратними ключами та паролем користувача зашифроване сховище ключів та секретної інформації (логіни / паролі). Воно має загальнодоступний API. Опція Non-Migratory (NM) дає можливість провести дешифрування тільки на пристрої, де дані були зашифровані. В икористовується унікальний ідентифікатор UID.

Резервні копії

Резервне копіювання можна виконати на ПК або в iCloud. Локальний бекап шифрується вибраним паролем, так формується структура Keybag. Ненадійний пароль не зв'язаний з апаратними ключами і тому має слабке місце, а сааме, не стійкий до брутфорсу (перебору варіантів). Зазвичай iOS використовує 10 млн. ітерацій PBKDF2, щоб підвищити стійкість до

переборів. При копіюванні в Apple iCloud дані шифруються Curve25519, це дозволяє зробити резервне копіювання навіть при заблокованому пристрої.

Зашифровані ключі за допомогою iCloud Keychain, стають відомими Apple, тому виробники чи шахраї можуть отримати доступ до бекапу. Додатково Keychain шифрує обидва типи резервної копії ключем UID, щоб запобігти передачі даних на сторонній пристрій. Резервному копіюванню в iCloud підлягають: дані додатків; резервні копії Apple Watch; настройки пристроїв; SMS і MMS, фото і відео; історія покупок в сервісах Apple; домашній екран і iMessage; пароль голосової пошти.

SEP: TouchID і FaceID

Secure Enclave Processor (SEP) — співпроцесор, який використовує зашифровану пам'ять і організує роботу з автентифікації, керуванню ключами, шифруванню и генерації випадкових чисел. Якщо ядро iOS було зламано, то SEP забезпечить шифрування за рахунок власної автономної архітектури.

Зменшення фронту атаки

При заблокованому пристрої обмежуються шляхи вводів і виводів даних і сааме це зменшує фронт атаки. Щоб доставити експлойт на пристрій Apple , треба пройти одним із таких шляхів:

- синхронізацію даних в фоновому режимі;
- пуш-повідомлення;
- деякі повідомлення з мережі (Wi-Fi, Bluetooth, стільниковий зв'язок);
- порт Lightning на пристрої.

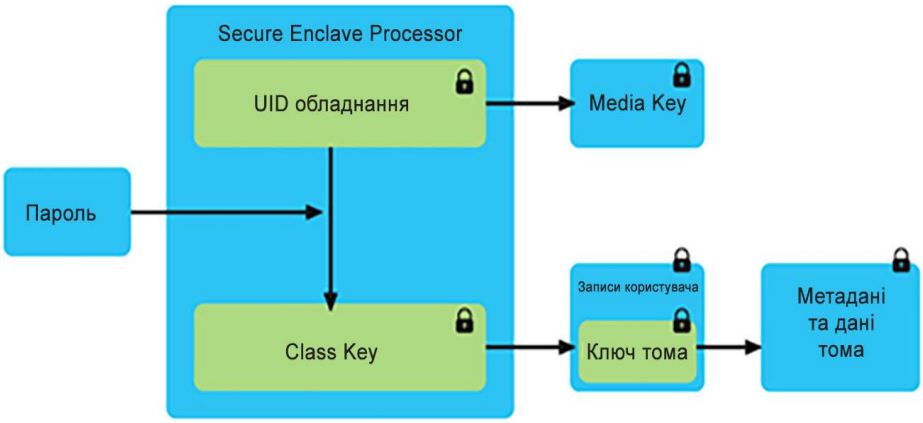


Рис. 3. Схема обробки ключа Secure Enclave Processor

Робота автентифікації TouchID / FaceID узгоджується через SEP.

Після введення USB Restricted операційна система почала обмежувати доступ несанкціонованих підключень через USB/Lightning, наприклад, інструментів комп’ютерної криміналістики. iOS зупиняє роботу USB після першого підключення, якщо пристрій не був зазначений користувачем, як довірений. Довірені підключення з використанням USB/Lightning залишаються в пам'яті на місяць.

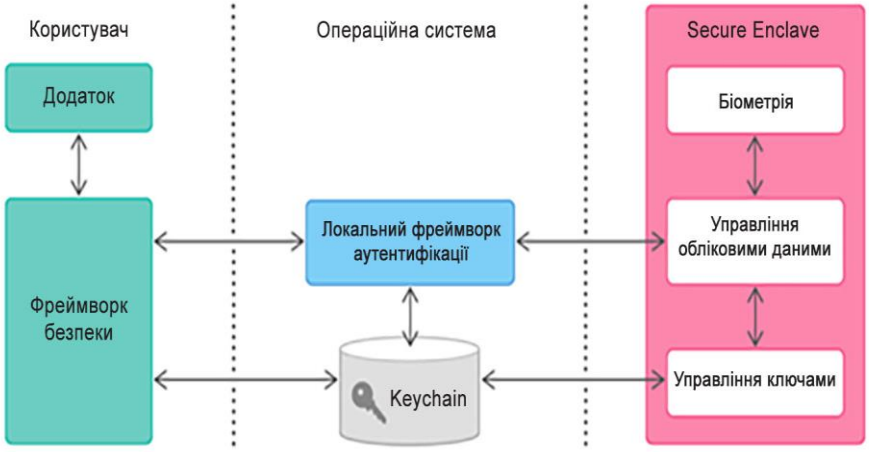


Рис. 4. Схема роботи Apple TouchID і FaceID

Message і FaceTime

За допомогою FaceTime, Apple підтримує наскрізне (end-to-end) шифрування відео- / аудіозв'язку між своїми пристроями. Дане шифрування базується на основі безпечного транспортного протоколу в режим реального часу(SRTP). В iMessage використовується схема шифрування «signcryption».

Публічні ключі використовують Apple Identity Service — як довірений орган, що доводить справжність користувачів.

Актуальні техніки обходу захисту користувацьких даних iOS

Як тільки в продажу з'являється нова серія пристроїв Apple з підвищеним рівнем безпеки, відразу ж вона стає цікавою для зловмисників, і фахівців з кіберкриміналістики і багхантерів, які отримують достойну платню за виявлення недоліків. Отже, назвемо кілька сучасних технік обходу захисту для iOS.

Джейлбрейк і програмні експлойти

Для усунення обмежень iOS найчастіше використовується джейлбрейк випускається під конкретний пристрій і версію iOS. Більшість інструментів криптоаналізу застосовує *Jailbreak* для доставки «корисного навантаження» в проблемний компонент програми, через USB/Lightning. Доставка здійснюється з допомогою повідомлень або спеціальних веб-сторінок. Ще користуються ланцюжком експлойтів. З початком контролю над ядром iOS , можна дістати зашифровані дані, Наступна модифікація (патчинг) програмного ядра дозволить запустити будь-який код в системі. Apple дбає про власну репутацію, тому вкрай швидко реагує на виявлення недоліків, які призводять до джейлбрейку, таким чином вдається тримати високу ціну сучасних робочих варіантів. Джейлбрейки checkm8 / checkra1n стали дуже ефективними в 2020 році в процесі кіберкриміналістичних досліджень, дозволяють працювати з пристроями до iPhone X в різних версіях iOS. Експлойти Cellebrite UFED Touch и 4PC – це можливість запуску резервного копіювання без авторизації користувача або активації загрузчика з кодом Cellebrite для вилучення частин файлової системи прист

Підбір паролю

Раніше зловмисники могли проводити більш успішні атаки за рахунок анулювання показників лічильника неправильно введених паролів, бо перевірка паролю контролювалася процесором самого пристрою. З появою архітектури SEP з'явилися обмеження на вгадування комбінації, і ймовірність зламу зменшилася В раніших версіях iOS для збою лічильника відключали живлення пристрою, а в 2016 році була застосована техніка віддзеркалювання флеш-пам'яті NVRAM на iPhone 5C і число вводу паролів стало необмеженим. (Табл.1) Обмеження на підбір в 80 мс робить

атаки з перебором безглуздими для складних паролів, що складаються з літері цифр. Для PIN-коду з 6 цифр, що використовується за замовчуванням, обмеження на вгадування є основною перешкодою.

Таблиця 1.
Оцінка часу перебору цифрових паролів в iOS

Довжина паролю	4 цифри	6 цифр	10 цифр
Всього варіантів	10^4 = 10 000	10^6 = 1 000 000	10^10
Всього використовується	9276	997090	-
80 мс/спроби очікування	12,37 хвилини 6,19 хвилини	22,16 години 11,08 години	~25 років
10 хв./спроба очікування	~70 днів ~35 днів	~20 років ~10 років	~200 000 років

Злам SEP

Для взаємодії с SEP необхідні привілеї ядра. Отже, *Jailbreak* – це складова частина ланцюжка для злому SEP. Якщо атака на SEP вдалася, то шахрай чи фахівець з кібераналізу мають необмежений доступ не тільки до ключів шифрування, а й до багатьох інших функцій захисту та можливість дістатися до інформації з будь якого файлу. Компанія Grayshift з 2018 р. винесла на ринок цікавий інструмент GrayKey, який ніби то зміг обходити обмеження SEP. Як доказ, було продемонстровано низку витоків інформації (вдалий злам пароля блокування екрану iPhone X). На початку 2020 року дізналися про витік з ФБР. За не підтвердженими даними GrayKey отримав доступ до заблокованого iPhone 11 Pro Max (iOS 13), невразливого для checkm8. Цей факт викликає появу багатьох питань, наприклад: чи було це робочим эксплойтом? Чи, може, це звичайна компрометація SEP?

Вилучення даних

Стратегічні плани вилучення даних бувають різні і залежать від того, включеним чи виключеним є пристрій на момент захоплення. Часто, коли відбувається конфіскація пристрою Apple, правоохоронці забирають також і суміжні пристрої MacBook чи Apple TV, щоб проаналізувати їх вміст, використовуючи клітку Фарадея або автономне джерело живлення для запобігання вимкнення приладів. У випадках, коли атаку на iOS, здійснюють зловмисники, останнім рубіжем захисту залишається шифрування від Data Protection. Тому витяг даних без згоди чи при відсутності користувача проходитиме по одному із трьох сценаріїв.

1. ***Доступ до приладу за допомогою ключів***. Ключі шифрування, що загрузилися в пам'ять, можна вилучити. Скажімо, інструменти криптоаналізу Cellebrite UFED і XRY Logical дають дозвіл підключитися до пристроїв iOS через порт USB/Lightning або через Bluetooth, а також здійснити резервне копіювання чи переглянути файли.
2. ***Обхід захисних механізмів***. Навіть недоступні для вилучення дані, в окремих випадках все ж вилучаються, з допомогою інструменту GrayKey. Він з успіхом справляється з завданням дешифрування кодів доступу користувача. Вдала високочастотна атака шляхом перебору паролю користувача дозволить вилучити всі файли iOS, Keychain і вміст iCloud. І результат не залежить від того в якому стані (AFU чи BFU) знаходився пристрій до початку атаки.
3. ***Альтернативні джерела даних.*** Застосовується атака на резервну копію iOS, що зберігається в локальному комп'ютері і має слабкий захист від брутфорсу. Також тут вилучаються дані користувача із хмарових сервісів.

Посилення захисту даних. Apple створила якісне програмне середовище (фреймворк) для захисту даних користувача, але поки Data Protection використовується в не дуже строгому режимі. Скажімо, токени автентифікації для хмарових сервісів можуть бути вилучені із пам'яті. Хоча клас захисту в стані AFU досить надійний але ретельнішої організації його роботи.

Динамічний захист даних. Досягається завдяки взаємодії з користувачем на основі навчальних алгоритмів разом з покращенням захисту до класу CP. iOS передбачає, які ключі і коли саме повинні бути застосовані. Неактуальні своєчасно видаляються з пам'яті, натомість вводяться нові.

Наскрізне шифрування бекапів і iCloud. Apple зберігає ключі, які дозволяють розшифрувати дані бекапів в iCloud. Під час використання iCloud Keychain, якісно організується наскрізне резервне копіювання, недоступне для Apple, але доступне для будь якого довіреного пристрою користувача. Це використовується і для контейнера CloudKit, та підвищує безпеку зберігання даних користувача в хмарі.

Паролі на локальні бекапи. Захистити від переборів, зможуть паролі локальних бекапів, які мають підвищену складність. Саме такі рекомендують створювати шляхом навчання користувача і оптимізації інтерфейсу.

Підсилення iCloud Keychain. Є ще одна слабинка це — кластер HSM, тому що відсутня прозорість шифрування зі сторони серверу. Apple зазвичай *застосовує технологію Certificate Transparency, це коли вузли перевіряють* адреси и коректність HSM, роблять інформацію публічною і діляться нею.

Обмеження на USB-інтерфейс. Строгіші обмеження під час керування USB/Lightning на рівні ядра iOS можуть підсилити безпеку і запобігати роботі експлойтів, наприклад, checkm8.

Обмеження на режими DFU і JTAG. Користувачі коли завгодно мають змогу перевести свій пристрій в режим DFU, і експлойти здатні використати цю шпаринку. Організується автентифікація з криптографією. Подібні рекомендації підходять і до режиму JTAG, хоча ним користується менша кількість людей.

Прозорість і функціональні протиріччя. З питань захисту користувацьких даних в Apple э протиріччя, які відразу треба усувати. Наприклад, включення / виключення опції синхронності даних з iCloud, заплутує користувача і з'являється ризик витоку даних. Те саме можна сказати і про інтерфейс, і про налаштування, і про управління iCloud за замовчуванням.

Компанія Google, операційна система Android

Android, або Android Open Source Project (AOSP), — це набір програмного забезпечення з відкритим початковим кодом, розробленим Open Handset Alliance під крилом Google. Мобільні сервіси Google (GMS), достатньо добре розширюють і ускладнюють систему Android, бо містять в собі пропрієтарні API и програмні сервіси. Зайнявши основну позицію на базі Linux, Android має всі переваги та недоліки безпеки даної ОС. Вразливість мобільних пристроїв Android завжди гостро відгукується у світі з огляду на популярність і поширення цих гаджетів.

Захист даних користувача Android на сьогоднішній день.

Автентифікація

Графічний ключ (патерн), цифровий код чи фраза із літер і цифр. Патерн-автентифікацію по силі прирівнюють до цифрового паролю з 2-3 цифр. Також іноді задіяна і біометрична автентифікація за відбитком пальця чи розпізнавання обличчя. Вона вводиться виробниками пристроїв за бажанням, бо для Android є не обов'язковою. Підключається опція Smart Lock, в цьому випадку для розблокування системою використовується інформація про оточення (телефон перебуває в сумці, лежить вдома).

Пісочниця для додатків

Застосовується дискреційний (вибірковий) контроль за доступом (DAC) и SELinux. Файли додатка мають дозвіл, який базується на ідентифікаторах користувачів Linux. Спроба відкрити не свій файл приведе до помилки. Додаткову ізоляцію забезпечує SELinux. Дана політика SELinux жорстко контролює привілеї додатків. Обов'язковий контроль доступ (MAC) дає змогу гарантувати, захищеність системи, навіть коли процес запуску проходить на правах суперкористувача (root).

Шифрування

Повне шифрування диску (починаючи з Android 4.4), коли задіяно модуль «dm-crypt» ядра Linux. Використовується алгоритм AES-128 в режимі CBC с ESSIV. Із паролю користувача створюється спеціальний ключ для шифрування майстер-ключа. Саме він має бути доступним під час загрузки

ОС, щоб активувати основні функції системи. Майстер-ключ використовується для всіх операцій блокування доступу до даних, тому після проходження користувачем автентифікації, назавжди залишається в пам'яті пристрою.

Файлове шифування — це так званий гранульований контроль. Модуль «fscrypt» ядра Linux використовує алгоритм AES-256 в режимі XTS для файлів CBC і для метаданих файлів. Маємо дві категорії зашифрованих файлів: Device Encrypted (DE) і Credential Encrypted (CE). Дані DE ввібрали в себе секрети пристрою та стають доступними і під час загрузки, і при розблокуванні, вони зарезервовані для системних додатків. Наприклад, для клавіатури, калькулятора, годинника, викликів). Дані CE шифруються ключем з паролю користувача і стають доступними тільки після розблокування. Використовуються всіма додатками за замовчуванням.

Android Verified Boot (AVB)

Тут застосований модуль верифікації «dm-verity», щоб перевірити цілісність початкової загрузки системи на основі криптографічного хеш-дерева. Перевірка завершиться помилкою, якщо під час загрузки модулів операційної системи одне із значень буде введено не правильно, а пристрій залишиться в нефункціональному стані. Підтримується і опція повернення до попередньої безпечної версії, яка зберігається в спеціальному розділі, стійкому до проникнення. Загружчик в позиції «розблоковано» дозволяє вимкнути AVB і ввести довільний код під час загрузки пристрою. Такий хід може знадобитися розробникам чи користувачам, якщо вони хочуть мати рут-доступ.

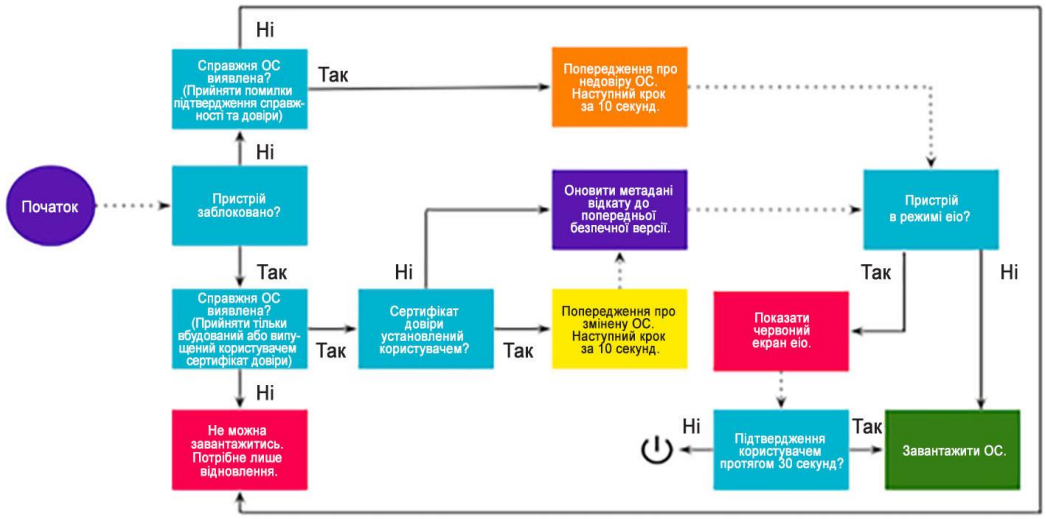


Рис. 5. Алгоритм роботи Android Verified Boot

Google Mobile Services (GMS)

Google користується Google Cloud для зберігання даних і протоколом TLS для зв'язку клієнтів з сервером. Дані із Google Cloud зашифровані з допомогою ключів, про які знає Google. Наскрізне шифрування підтримується тільки у програмі Google Meet. Розробники додатків співпрацюють з GMS через Play Services API. Є ще й API SafetyNet, така служба перевірки пристроїв Android на наявність рут-прав чи сумнівного ПО.

Підписування APK та перевірка коду

AOSP вимагає щоб розробник підписував створений ним додаток, який планується запустити. Підпис файлу APK відповідає відкритому ключ. Вони поширюються разом. До початку публікації додатку в Play Store відбувається автоматична і ручна перевірка коду співробітниками Google. В версії Android 11 уже задіяний модуль «fs-verity», який постійно перевіряє файли APK. При наявності сертифікату GMS телефон має опцію установки додатків з «невідомих джерел», відсутніх, наприклад, в Play Store або від інших розробників.

Резервне копіювання

З допомогою GMS, воно організоване 2 способами. Android Backup Service запроваджено в версії Android 2.2. Цей додаток створює копії пар ключів і значень відповідно до того, як їх розмістив користувач. Така опція не обов'язкова, вона закладається і налаштовується розробниками. В Android 6 вже працює механізм автоматичної синхронізації даних з Google Drive – Auto-Backup. Цей варіант обходиться без налаштування розробника, а користувач має змогу відмовитися від послуги. З 2018 року діє наскрізне шифрування для Android Backup Service. Ключ для шифрування бекапів створюється на пристрої, щоб дістатися до ключа, використовують класичну схему (PIN-код, пароль чи патерн). Дані додатків копіюються в сервіс Google Drive окремо, так як Android Auto-Backup. Вони шифруються паролем акаунту Google чи автентифікацією користувача на пристрої. У Google є доступ до цих ключів. Іноді виробники пропонують власні бекап сервіси. Android Debug Bridge та інші інструменти, що дозволяють робити резервне копіювання на комп'ютер через USB.

Техніку обходу захисту даних користувачів Android

Root-доступ і використання експлойтів**.** Отримання root-доступу в Android подібне до *Jailbreak* на iOS — це дозволяє модифікувати ОС відповідно до потреб користувача, оминати обмеження виробників чи запускати довільний код. Бувають пристрої, які користуються root-доступом для розблокування, тоді необхідно розблокувати загружчик. Всі користувацькі дані при цьому видаляються, бо система перестає довіряти загрузці і не може гарантувати безпеку. Але є такі експлойти, що дозволяють обходити ці обмеження. Згідно зі статистикою SafetyNet від 2017 року, 5,6 відсотків Android пройшли процедуру рутування. Починаючи з 2013 р. Samsung запровадив запрограмований електронний запобіжник Knox-bit. Він спрацьовує під час спроби рутування, виходить з ладу і може бути замінений тільки апаратно. Google SafetyNet також відстежує пристрої, де було застосовано root-доступ. Отже, техніка блокується виробниками. Різними способами отримується root-доступ за допомогою експлойтів без видалення даних користувача (атака на ядро ОС чи код OEM або особливості SoC). Android базується на ядрі Linux, проблемні місця у них спільні і дозволяють використати доступ суперкористувача. На вразливості Linux Dirty CoW базується експлойт під Android, а прогалина PingPongRoot, в ядрі Android, може використовуватися в Linux. Продовжують виявлятися ще і нові невідомі досі недоліки (0-day), що можуть забезпечити root-доступ. Атака на конкретний пристрій вузько спрямована. Враховуються особливості прошивки компонентів, обладнання, якщо проводять маніпуляції, то можлива загрузка інтерфейсу Qualcomm EDL, а не Android. Таким чином шахрай записує потрібний код в розділ Android і отримує права суперкористувача без втрати даних Рутування можливе і за допомогою інструменту SP-Flash-Tool без розблокування загружчика, якщо на пристрої присутні компоненти MediaTek. Список досить великий.

Як можна було б підвищити захист Android

Шифрування даних користувача під час блокування екрану

Ключ шифрування видаляється з пам'яті після блокування екрану. Особисті дані будуть недоступні до того часу, поки користувач не ввімкне пристрій. Така функціональна особливість Android підвищить рівень безпеки на порядок але розробникам доведеться адаптувати роботу додатків в фоновому режимі із заблокованим екраном. Це також обмежить ефективність вилучення даних із рутованих через експлойти приладів.

Запровадження наскрізного шифрування для продуктів Google

Підвищить безпеку даних і довіру користувачів наскрізне шифрування в службах GMS. Хоча треба пам'ятати, що така надійна конфіденційність, може перешкоджати правоохоронцям отримувати цінну інформацію для боротьби з небезпечними злочинцями.

Безпечний доступ в роботі з прошивкою

Більшість експлойтів здатні обійти захисні механізми Android, користуючись недоліками в прошивці. Існує два шляхи вирішення питання: апаратний спосіб, коли розповсюджуються

програматори прошивки з компонентами, захищеними від проникнення і вони дозволять відслідковувати витік. Другий варіант — відкликати сертифікат скомпрометованого програматора.

Підсилення компонентів апаратної частини

Функціональність TEE TrustZone підсилюється апаратно, коли використовується співпроцесор безпеки. Виробники не завжди йдуть на такий крок, бо додатковий співпроцесор не дозволить зменшити вартість пристрою.

Підвищення частоти оновлення Android

Сьогодні пристрої мають дуже надійний захист даних користувача. Але остання версія ОС встановлена далеко не на всіх пристроях, тому ризик проникнення залишається досить високим. Особливо це стосується застарілих варіантів, коли просто неможливо провести оновлення операційної системи. Знизити відсоток ризику допоможе запровадження навчання користувачів і своєчасне оновлення ОС.

Переваги відкритого коду і екосистеми

Швидке та ефективне захоплення ринку та популярність Android у світі допоможуть підвищити захист. Дякуючи відкритому коду, розробники вводять покращені оновлення незалежно від Google. А Google може формувати стандарти безпеки та просувати різні протоколи. Цілісне ядро Linux і Android взаємовигідне для обох платформ. Оскільки, вони допомагають один одному вчасно виявляти і ліквідовувати проблеми, поступово підвищувати безпеку.

Особливості безпеки Apple iOS:

- Автентифікація користувача (цифровий PIN-код, пароль, біометрія) + SEP;
- підписування коду (Boot ROM і підписування додатків);
- пісочниця і аналіз коду додатків;
- шифрування (AES, ECDH over Curve25519, UID, Data Protection classes);
- Keychain (API для безпечного зберігання ключів);
- Резервне копіювання (Keybag і iCloud Backup Keybag);
- хмаровий сервіс iCloud і CloudKit (API для iCloud);
- iCloud Keychain (синхронізація і відновлення Keychain);
- апаратна безпека (SEP);
- контроль і обмеження фронту атаки (Wi-Fi, Bluetooth, пуш-повідомлення, USB/Lightning).

Особливості безпеки Google Android:

- Автентифікація користувача (цифровий PIN-код, пароль, патерн, біометрія) + Gatekeeper і Smart Lock;
- пісочниця додатків (DAC + SELinux);
- шифрування всього диска и файлів (AES-128/256, Credential Encrypted і Device Encrypted), а також SD-карти;
- Trusted Execution Environment (TEE) і додатковий апаратний модуль безпеки (secure element);
- Android Verified Boot;
- Резервне копіювання (Auto-Backup і Backup Service);
- Google Mobile Services;
- Підписування додатків і аналіз коду;
- Наскрізне шифрування в Google Meet.

Висновки

Зловмисник може проникнути систему і отримати конфіденційні дані, не залежно від використовуваної платформи, якщо докладе немалих зусиль. В кожній ОС є свої особливості безпеки.

Хоч Apple краще організує шифрування файлів на пристроях і в хмарі, ніж Google, виникають ситуації, коли шахраєві вдається отримати дані користувача. Зберігання токенів автентифікації для iCloud в режимі AFU треба переробити. Наскрізне шифрування всіх даних в хмарі, усуне

протиріччя в політиці конфіденційності Apple. Наскрізне шифрування рекомендують і для Android GMS. Серйозним недоліком Android є постійне зберігання ключів шифрування в пам'яті пристрою після першого розблокування. Аналог iOS Complete Protection збільшить захист даних користувача від шахрайських атак. Користувачам мобільних пристроїв рекомендують створювати дуже складні паролі разом з біометричною автентифікацією скрізь, де тільки можливо. Якщо є необхідність, то запроваджувати 2FA (двофакторну автентифікацію). Краще не закладати в хмару нічого зайвого і для цього треба гарно вивчити схему синхронізації даних з хмаровими сервісами. Рутирування/джейлбрейк приладів — це ризик запуску довільного коду (навіть в прошивці) і загроза виходу з ладу ОС пристрою. Сучасна безпека даних користувача на обох платформах організована досить якісно але і для Google Android, для Apple iOS є ще куди рости в цьому плані.

References

1. Wenbo Mao, “Modern Cryptography”, First Edition, Pearson Education, 2008 ISBN-. 13: 978-0132887410
2. Quisquater, J., Math Rizk, Side Channel Attack - State of the art, (2002).
3. Cetin Kaya Coc, Cryptographic Engineering/ Cetin Kaya Coc// Springer Science+Business Media, LLC 2009 – 171 p
4. Apple Platform Security. May 2022 available at: https://support.apple.com/guide/security/welcome/web (accessed 21 October 2022).
5. Secure Android devices. available at: https://source.android.com/docs/security (accessed 12 November 2022).

УДК 004.421.4

TEAM BASED PLAYER RANKING ALGORITHMS

DOI 10 36994 / 2788- 5518- 2022-02-04-22

Sergii Suglobov. *Open International University of Human Development "Ukraine",Kyiv, Ukraine. s.suglobov@gmail.com*

Anatolii Tymoshenko, *Ph.D., Ass. Prof. Open International University of Human Development "Ukraine",Kyiv,Ukraine. timoshag@i.ua*

Abstract: *The article considers algorithms for assessing the personal capabilities of players that are suitable for multiplayer online games with teams. Analyzed popular algorithms and proposed changes to adapt them work with teams of multiple players.*

Key words*: rating system, matchmaking*

АЛГОРИТМ ПІДРАХУНКУ РЕЙТИНГА ГРАВЦІВ В КОМАНДАХ

Суглобов С.В*. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. s.suglobov@gmail.com*

Тимошенко А.Г., *к.т.н.., доц. Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна.*

Анотація*: У статті розглянуто алгоритми оцінки особистих можливостей / рейтингу гравців, які підходять для багатокористувацьких онлайн-ігор з командами. Проаналізовані популярні алгоритми та запропоновані зміни (для алгоритмів що не підтримують команди), щоб адаптувати їх для роботи з командами з кількох гравців. Зроблено акцент саме на використанні алгоритмів для командних ігор. Алгоритми розглядаються по часу їх створення, так як кожен наступний алгоритм це покращена версія попереднього. Але при цьому кожен із цих алгоритмів використовується в сучасних іграх так як всі вони мають свої переваги. Рейтингові алгоритми в своєму загалі використовують два показники щоб оцінити гравця, рейтинг – це реальний рейтинг гравця котрий змінюється після кожної гри, та сігма – це відхилення від рейтингу яке показує наскільки ми можемо вірити в точність рейтингу, чим менше значення сігма тим точніше рейтинг гравця. Рейтинг змінюється після кожного матча в залежності від результата, якщо виграш то збільшується, в разі програшу то знижується. Сігма ж зменшуватися з кількістю ігор котрі гравець зіграв, тим самим підтверджувати реальний рейтинг гравця, або збільшуватися але з часом, тобто з часом зростає неточність рейтингу гравця. Для урахування рейтингу системою підбору зазвичай зручно мати представлення про рейтинг одним числом, в випадку якщо рейтинг представлено двома числами, тоді його обчислюють як рейтинг – 3* сігма. Таким чином беруть сильно песимістичне представлення про рейтинг гравця. Представлена порівняльна таблиця розглянутих алгоритмів.*

Ключові слова: *рейтингова система, пошук партнерів*

Introduction

Why do we need player ranking in the game?

- To make game fair enough for players which are added to one game session. Teams should have close summary ranking to each other. Close - is not mean that they should be identical, no, but to some extend so we can calculate that they have at least some chances of winning.
- To ensure teams balance in game session all chosen players for the game session splitting +/- equally on teams, that's also should be done based on each player ranking.

Ranking of a player should be corresponding to player performance in game or his real skills. Skill is tricky especially in shooter games when it depends on player reaction, practice, play time and

even some bit of luck. But still, skill can be measure as rough approximation of player abilities. What we really interesting is who's better than whom in our particular game. If a player has a higher rating than we expert him to win against player with lower rating. That give us a scale where every player has a rough approximate number which we can use for comparison.

Player ranking and they intersection can be visualized using Gaussian curve when every player can be described by two values: mean (rating), that representing skill difference and standard deviation, that representing probability of difference. If players intersect within borders of their respective deviations than we can say that they are compatible to play together (fig.1).

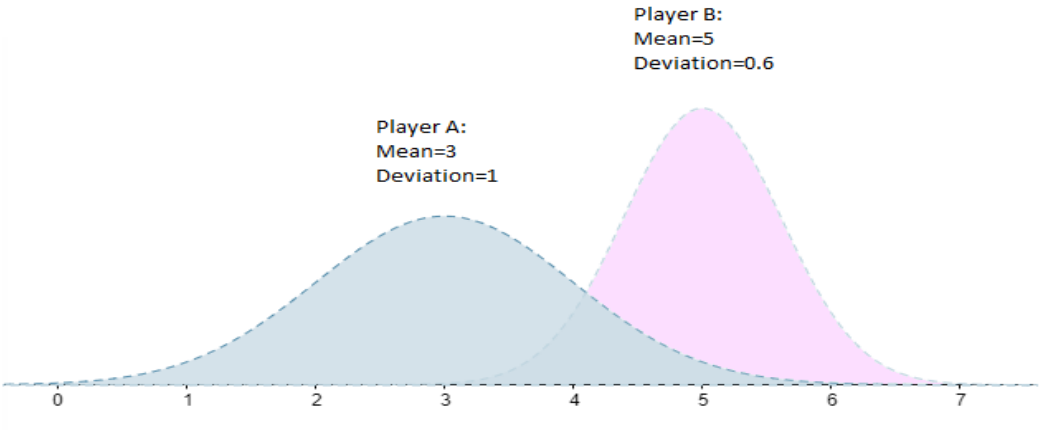


Fig. 1. Illustration of two player ratings

Goal of ranking algorithms is to give players a fun and enjoyable game when he have a challenge and some probability of winning. Knowing player skills, we can predict rough probability of winning in the match. Good metric here can be used a 50% win rate in total number of matches.

Simple solution that also can be used for some purpose.

Research

Win – Lose. Every of presented algorithms use game outcome as main parameter for creating player rating. Simplest way to differentiate player ranking based on win/lose outcome of game session can be calculated:

$$R_{new} = R_A + S_T \ , \tag{1}$$

S_T – it is a match result of player team, win counts as 1, a loss as -1 and draw as 0**.**

Matching player among each other can be done by determining allowed distance between they ranks as 200 (value should be based on statistic) when probability of winning is not less than 60%(fig.2).

Pros:

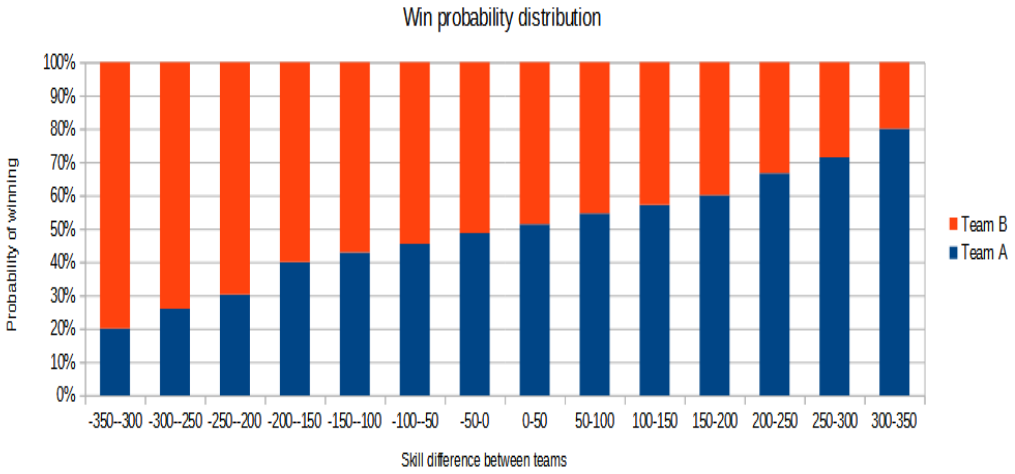
- Easy to implement that can be great for game development time.
- It is enough to disperse players on groups with some distance from each other that allows matchmaking to do it's job. Players that play better will go higher and less skilled player go down. In result you should
- ave probability of winning as visualized on the next picture:

* negative skill difference mean that advantage to Team B (positive for Team A)

Cons:

- Big spreading with time.
- Slow adaptation for player ranking. Rank always change monotonically by 1 point.

- Has no control on rank scaling.
- Does not take into account player personal performance. It will be worse in situation when players play as part of group and other players of the group play much better. Even if one of the players always with the lowest score, his overall skill can be high.
- Does not take into account time of playing in the match. Not every player play from the start of the match.
- Does not change with time when player don't played the Game for long period of time. In this case player rating become unreliable.



Fig, 2. Win probability distribution

Elo. Key ideas of Elo rating system:

- Developed mainly as rating system for two players (like a chess, but can be used for many match-ups with some modifications.
- Operated by only one storable parameter known as rating (R) that should describe player skill. Initial rating recommended to set = 1500, but also it can be any other value even 0.
- Rating calculated in two steps:
- Calculating expected result (E) of the Game based on known player ranks. It get us a normalized value from 0 to 1 of a chance to win.
- Calculating update for player ranks based on the expected result and game outcome or final score (S).

- Let's take a closer look at the math behind Elo. Imagine that we have two players: A with rating 120 and B with rating 80. Expected result of this match can be calculated by the formula:

$$E = \frac{1}{1+10^{(R_B - R_A)/D}} \ , \qquad (e.1)$$

R_A – rating of the player for which expected result is calculating; R_B – rating of the opponent:

$$E_A = \frac{1}{1+10^{(80-120)/400}} \approx 0.56 \ .$$

It is mean that player *A* probability to win the game is 0.56. If we calculate the same for Player *B* we will have probability = 0.44 of winning.

D – ratio of difference, that known in Elo as mysterious 400 number. It should be chosen as difference between players with which one player will have 10 times more chances to win the game. A player with double *D* rating (800 points) over another player have 100 times better chances to win.

D number is arbitrary, if you want a wider range of possible rankings, increase the value, if you want a narrower scale, decrease it.

Let's calculate new rating for player *A* using formula (also assume that player is a winner):

$$R_{new} = R_A + K(S_A - E_A)\ , \qquad \text{(e.2)}$$

$R_A = 120 + 10(1 - 0.56) \approx 124$;

S_A – final score, it is an actual result of the game when win=1, loss=0, draw=0.5.;

K – is known as the k-factor, or development coefficient.

It usually take values started from 2 to 40. It determines how a result affects the rating of players after the game. The higher the value the more change to the rating it brings. In our example we use k-factor equal to 10 and it give player A increase in 4 point to rating, in case of K=20 it will be 8 points. It can be a good idea to use higher coefficient for new players as they tend to improve faster and lower coefficient for all other players. If your game has many game sessions than it's better to use lower K to prevent measures from changing by large amount.

At the end of the game Player A rating rises by 4 point to 124 while Player B rating falls by the same number of point to 76.

The Elo rating system measures the relative strength between players when calculating players rating. If Player A had lost that game than his rating would have fallen by 6 points and Player B will increase his skill by 6 point. It does make sense, as Player B should be rewarded with more points for winning to more skilled player even when he is expected to lose.

Elo rating system work well for estimation player rating and we can use it to combine each players ratings to create a team rating. Unfortunately, Elo only knows how to compare two players at a time. So, first of all let's adapt it to multiplayer game with two teams by changing logic of estimation player skill to match every player of one team to every player of opponent team ($Team_{A1}$ vs $Team_{B1-BN}$). A game with teams of the same size has N(N-1)/2 distinct pairwise matching of player against team opponents.

Expected score in this case can be calculated using the formula:

$$E_A = \frac{\sum_{n=1}^{N}\left(1+10^{(R_n - R_A)/D}\right)^{-1}}{N(N-1)/2}\ , \qquad \text{(e.3)}$$

N – it is a number of players in team,

R_N – every player in opposite team.

Actual score can be calculated in the same way as an original Elo proposed, winner team get 1 and losing team get 0. If we do it like this than every player of team get the same amount of points. Just like simple Win-Lose algorithm except number of points can be different because of K value. It is not fair for players which performed the most.

Let's think about conditions to calculate actual score that include personal performance of a player:

- All players of winning team should increase their score as well as all score of the losing team should be decreased.
- Scores of players in each team should be decreasing monotonically. 1st place has a higher score than 2st place.
- Personal score representing the actual rank in team at the end of the match, is normalized so that the ranks of players in team sum up to 1.

Based on this condition let's write the formula for calculating final score:

$$S_A = S_T + \frac{N - Pl_A}{N(N-1)/2} \quad , \tag{e.4}$$

S_T – it is a match result of player team: win=1, loss=0, draw=0.5,
Pl_A – it is a place of a player in his team in final score board (1 for 1st, 2 for 2nd, …, *N* for last).

Played time it is one more parameter that can be included in skill calculation. There is many possibilities in online games and one of them that team players in game session can be added in the middle of a game as well as for the end of the game session. In this case it is incorrect to calculate player score that can be 0. To avoid this situation we can add an additional variable for calculation:
$\hat{t}$ - normalized version of minutes or seconds played by the player.

$$\hat{t} = \frac{t}{S_t} \quad , \tag{e.5}$$

t – time played in the game session by player,
S_t – total time of the game session.

Final formula for calculating new player ranking should be look like:

$$R_{new} = R_A + K\hat{t}(S_A - E_A). \tag{e.6}$$

Seems everything is fair:

- Player 24 was expected to have the best performance that's why got the biggest rating decline because of loss and bad scoring.
- Player 25 was expected to have lowest performance that's why got the lowest rating decline because of loss

Glicko. The Glicko rating system extends Elo system by adding to it - rating deviation (RD). Therefore rating system operated by three storable parameters player rating, rating deviation which measures the uncertainty in a player rating and latest rating update to find out time period.

Main difference from Elo is that player rating changes not only because of number of matches played but rating changing with time.

How rating deviation works:

- Than lower RD than more certain that rating of a player is accurate. The RD increase slowly over time of inactivity.
- Than lower RD than slower changing rating of a player. That allows for fast adaptation for player rating from the start and after that it not change so dramatically.
- RD takes meaning from 30 (recommended to not use the RD lower than this value to ensure rating can change appreciably even in a relatively short time) to 350 (assumed to be the RD of an unrated player).

Where **c** is a constant that based on the uncertainty of a player skill over a certain amount of time. It assumes how many rating periods would take for a player rating deviation to return to an initial uncertainty of 350. For example, let's suppose that one rating period it is a one month of a playing and assume that after 5 years (or 60 rating periods) we will be uncertain about player skill. Also suppose that typical player has RD = 50.:

$$c = \sqrt{(350^2 - 50^2)/60} \approx 44.72 \quad . \qquad \text{(g.1)}$$

Where **t** is the amount of rating periods since player was in the Game. For online game we can decide that if player played at least once in the latest month than it is 0, and with every month that he doesn't play it is +1. Let's calculate RD=50 for different t (t=1 mean player doesn't played more than a.

Table1.
Elo rating calculation for 2 teams (K=10)

Player	R	E	Game Score	R_{new}
Team A (win – ratings go up)				
Player 11	1800	0.68	3500	1802.6 (+2.6)
Player 12	1700	0.57	2200	1702.8 (+2.8)
Player 13	1650	0.52	2100	1652.7 (+2.7)
Player 14	1850	0.73	1200	1851.6 (+1.6)
Player 15	1140	0.13	1100	1143.7 (+3.7)
Player 16	1500	0.37	720	1502.5 (+2.5)
Player	R	E	Game Score	R_{new}
Team B (loss – ratings go down)				
Player 21	1800	0.68	2000	1798.6 (-1.4)
Player 22	1750	0.62	1800	1748.5 (-1.5)
Player 23	1600	0.466	1800	1598.9 (-1.1)
Player 24	1850	0.73	1200	1847.6 (-2.4)
Player 25	1100	0.106	1100	1099.8 (-0.2)
Player 26	1500	0.37	750	1498.5 (-1.5)

The Player A current RD should be determined :

$$RD = min\left(\sqrt{RD_A^2 + c^2 t}, 350\right) \qquad \textit{(g.2)}$$

month) using formula g.2:

Table 2.
Calculating RD with different t

t=0	t=1	t=2	t=3
50.0	67.08	80.62	92.2

```
from collections import namedtuple

P = namedtuple('PlayerInfo', ['rating', 'score'])
D = 400
K = 10

winning_team = [P(1800, 3500), P(1700, 2200), P(1650, 2100),
            P(1850, 1200), P(1140, 1100), P(1500, 720)]
losing_team = [P(1800, 2000), P(1750, 1800), P(1600, 1800),
             P(1850, 1200), P(1100, 1100), P(1500, 750)]


def calc_for_team(team: list[P], opponent_team: list[P], win=True):
    team_size = len(team)

    new_ratings = {}
    for player in team:
        place_in_team = sorted(team, key=lambda p: p.score, reverse=True).index(player) + 1
        personal_score = (team_size - place_in_team)/(team_size*(team_size - 1)/2)
        expected_scores = [(1 + 10**((op.rating - player.rating) / D))**-1
                           for op in opponent_team]
        actual_scores = [K * ((1 if win else 0) + personal_score - e)
                         for e in expected_scores]

        new_rating = player.rating + round(sum(actual_scores) / (team_size * (team_size -
1)/2), 1)
        new_ratings[player] = new_rating

    return new_ratings


if __name__ == '__main__':
    print("Winning team:")
    for player_, rating in calc_for_team(winning_team, losing_team, win=True).items():
        print(f" {player_} rating become {rating}")

    print("Losing team:")
    for player_, rating in calc_for_team(losing_team, winning_team, win=False).items():
        print(f" {player_} rating become {rating}")
```

Table above shows how RD increasing over a time.
Next step is to calculate expected score between two players:

$$E_A = \left(1 + 10^{-g(R_A - R_N)/D}\right)^{-1} \quad , \qquad \text{(g.3)}$$

D=400 – ratio of difference, the same as in Elo,
R_A – is the player's rating,
R_N – is the opponent's rating.
g – is a function that calculated by the formula:

$$g = \frac{1}{\sqrt{1+3q^2RD^2/\pi^2}} \quad , \tag{g.4}$$

q – is a constant which is equal to log(10)/D = 0.0058565.

Before new rating is calculated, the new RD is needed to calculate for the player:

$$RD_{Anew} = \frac{1}{\sqrt{1/RD^2+1/d^2}} \quad , \tag{g.5}$$

where d^2 calculated as:

$$d^2 = \frac{1}{q^2g^2E(1-E)} \quad . \tag{g.6}$$

Having expected score, game session outcome and new RD we can find out updated rating using formula:

$$R_{Anew} = R_A + qRD_{Anew}^2 g(S_A - E_A) \quad , \tag{g.7}$$

S_A – is the outcome of the Game session: win=1, loss=0, draw=0.5.
Glicko as well as Elo designed to work only with two players, so we need to adapt it to work with teams, just like we do for Elo. In the simplest way we just need to sum up rating and rating deviation for every player of the Team i with every player in Team j and than divide on number of player in teams. For two teams of the same size calculation of rating and rating deviation can be wrote like:

$$RD_{Anew} = \frac{\sum_{1\le j\le N}\left(\sqrt{1/RD^2+1/d^2}\right)^{-1}}{N_T} \quad , \tag{g.8}$$

$$R_{Anew} = \frac{\sum_{1\le j\le N} R_A + qRD_{Anew}^2 g(S_A - E_A)}{N_T} \quad , \tag{g.9}$$

N_T – is the number of player in one team.
Let's get two teams and calculate ratings for them:

TrueSkill

The TrueSkill rating system is also generalization of the Elo system, developed by Microsoft Research and has been patented (no free license) and used for Xbox games. System additionally to rating tracks the uncertainty about player rating, can deal with any number of teams (even with asynchronous team sizes) and can infer individual skills from team results.

The TrueSkill more adapted to multiplayer online games with teams of many players including:

- Individual player skill for every team member. Team wins but player own skill needed for further matchmaking.
- Partial play that allows to handle situation where a player wasn't present for the entire game ssesion. Implemented as weighted sum factor where the weights are the percentage of the time player was present.

Table 3.
Glicko rating calculation for 2 teams

Player	R	RD initial	t	RD	g	E	d^2	RD_{new}	R_{new}
Team A (win – ratings go up)									
Player 11	1662	290	0	290	0.736	~0.43	499.04^2	249.74	1812.0
Player 12	1746	252	0	252	0.781	~0.51	469.47^2	220.98	1851.66
Player 13	1794	100	1	109.46	0.945	~0.57	402.07^2	105.35	1819.4
Player 14	1823	50	2	66.95	0.969	~0.61	399.15^2	78.68	1836.26
Player 15	1842	30	0	30	0.995	~0.63	403.81^2	30	1843.84
Player 16	1500	350	0	350	0.669	~0.30	585.90^2	299.81	1743.31
Team B (loss – ratings go down)									
Player 21	1662	290	0	290	0.736	~0.43	499.04^2	249.74	1547.83
Player 22	1746	252	0	252	0.781	~0.51	469.47^2	220.98	1632.1
Player 23	1794	100	2	118.17	0.936	~0.57	402.07^2	113.12	1754.08
Player 24	1823	50	3	91.9	0.960	~0.61	399.15^2	89.41	1795.82
Player 25	1842	30	0	30	0.995	~0.63	403.81^2	30	1838.72
Player 26	1500	350	0	350	0.669	~0.30	585.90^2	299.81	1396.98

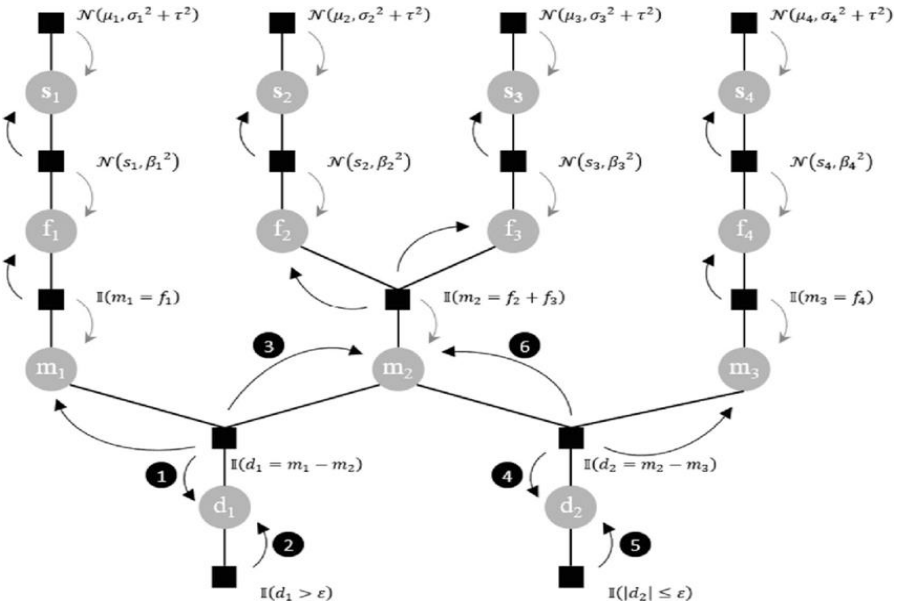
From the first look on factor graph it is hard to understand how skills should be calculated. That is why we will try to explain TrueSkill without it but in straight forward way.

As well as Glicko rating system TrueSkill system assumes that the skill represented a Gaussian distribution when each player satisfies a normal distribution of **mean μ** and **variance σ**, which are fixed to be the same for all players at the initiate step: $\boldsymbol{\mu}_{\mathbf{initial}} = 25$, $\boldsymbol{\sigma} = 25/3$ and $\boldsymbol{\beta} = \sigma/2$. The parameter β controls the updating effect, larger β leads to a more dramatic changes.

```
import math
from collections import namedtuple

P = namedtuple('PlayerInfo', ['skill', 'rd', 'score', 't'])

D = 400
RD_MAX, RD_MIN, RD_TYPICAL = 350, 30, 60
RT_AWAY = 60

c = math.sqrt((RD_MAX**2 - RD_TYPICAL**2)/RT_AWAY)
q = round(math.log(10)/D, 7)

winning_team = [P(1662, 290, 3500, 0), P(1746, 252, 2200, 0), P(1794, 100, 2100, 1),
            P(1823, 50, 1200, 2), P(1842, 30, 1100, 0), P(1500, 350, 720, 0)]
losing_team = [P(1662, 290, 3500, 0), P(1746, 252, 2200, 0), P(1794, 100, 2100, 2),
            P(1823, 50, 1200, 3), P(1842, 30, 1100, 0), P(1500, 350, 720, 0)]

def calc_rd(rd_initial, time_periods_away=0):
   return min(math.sqrt(rd_initial ** 2 + c ** 2 * time_periods_away), RD_MAX)

def calc_g(rd):
   return 1/math.sqrt(1 + (3 * q**2 * rd**2)/math.pi**2)

def calc_expected_score(g, player: P, opponent: P):
   return 1/(1 + 10 ** ((-g * (player.skill - opponent.skill)) / D))
```

```
def calc_new_rating(r, rd_new, g, s, e):
   return r + q * rd_new**2 * g * (s - e)

def calc_for_player(player: P, opponent_team: list[P], win=True):
   rd = calc_rd(player.rd, time_periods_away=player.t)
   g = calc_g(rd)
   expected_scores = [calc_expected_score(g, player, p)
                      for p in opponent_team]
   rd_x = [calc_rd_new(rd, calc_d2(g, e)) for e in expected_scores]
   ranking = [calc_new_rating(player.skill, rd, g, (1 if win else 0), e)
              for rd, e in zip(rd_x, expected_scores)]
   rd_new = sum(rd_x)/len(opponent_team)
   r_new = max(sum(ranking)/len(opponent_team), RD_MIN)
   return r_new, rd_new
```

The TrueSkill express the model as a factor graph and use approximate message passing to infer the marginal belief distribution over the skill of each player. An example of it:



Fig, 3. TrueSkill factor graph example

The Player current sigma (**σ**) should be determined by using formula:

$$\sigma = \sqrt{\sigma^2 + \tau^2} \quad . \tag{t.1}$$

Where **τ** is the dynamic factor which restrains a fixation of rating. The recommended value is percent of sigma: σ/100.

Updating mean value calculation after game session shown below:

$$\mu = \mu + S_T \left(\frac{\sigma^2}{c}\right) \upsilon\left(\frac{t}{c}\right) \ , \tag{t.2}$$

S_T - is the outcome of the Game session for your team: win=1, loss=-1:

$$t = \mu_{winner} - \mu_{loser} \quad , \tag{t.3}$$

$$c = \sqrt{\left(N_S \beta^2 + \sigma_{winner}^2 + \sigma_{loser}^2\right)} \ , \tag{t.4}$$

N_S – it is a total number of players in game session:.

$$\upsilon(t/c) = \frac{N(t/c)}{\Phi(t/c)} \tag{t.5}$$

N and Φ represent the PDF and CDF of a standard normal distribution, respectively.

Updating sigma new value calculated by formula:

$$\sigma = \sqrt{\left(\sigma^2 \left(1 - \frac{\sigma^2}{c^2} \omega\left(\frac{t}{c}\right)\right)\right)} \quad , \tag{t.6}$$

where:

$$\omega\left(\frac{t}{c}\right) = \upsilon\left(\frac{t}{c}\right)\left(\upsilon\left(\frac{t}{c}\right) + t\right). \tag{t.7}$$

TrueSkill was the first algorithm documentally applicable to team games. TrueSkill sums the ratings of team members to calculate the rating of their team. Most of the ensuing rating systems leveraged a similar approach in their calculations. Calculation result for two teams:

Table 4.
TrueSkill rating calculation for 2 teams

Player	μ	σ	μ_new	σ_new
Team A (win – ratings go up)				
Player 11	40	2.10	40.158	2.09
Player 12	55	3.30	55.389	3.29
Player 13	35	1.25	35.056	1.25
Player 14	25	6.10	26.33	5.96
Player 15	33	5.92	34.25	5.79
Player 16	25	8.333	27.48	7.96
Team B (loss – ratings go down)				
Player 21	45	1.50	44.92	1.50
Player 22	60	1.30	59.94	1.30
Player 23	30	3.25	29.62	3.23
Player 24	20	5.10	19.07	5.02
Player 25	33	5.92	31.748	5.79
Player 26	25	8.333	22.52	7.96

- Player 16 & Player 26 are newbies and we can saw that they have more rating change than everyone else. This means the algorithm try to quickly adapt player to reasonable approximations of skill.
- Player 13 got the lesser change to rating because of the lowest value of sigma.

Weng-Lin

Weng-Lin or the OpenSkill rating system is similar to TrueSkill.
They propose to use generalized approach with different distribution models for different purposes. It is developed specially for online games with multiple teams, this algorithm aims to be simpler and faster than TrueSkill while yielding similar accuracy. Also it is distributed under free license.

Can be used with distribution models, like:

- Bradley-Terry - follow a logistic distribution over a player's skill, similar to Glicko.
- Plackett-Luce - generalized Bradley-Terry model for k ≥ 3 (k-number of teams participating in a game).
- Thurstone-Mosteller - models follow a Gaussian distribution, similar to TrueSkill.

Rating system assumes that skill represented by two value of **mu** (=25) and **sigma** (=25/3). We will skip the review of formulas this time, because this rating system includes several models and therefore deserves a separate article with an overview of mathematics and approaches. Limiting ourselves to results that can be obtained using, for example library [10].

Every of observed algorithms can be suitable for modern game. The most advanced are the algorithms of TrueSkill, also the most famous and OpenSkill (Weng-Lin) that looks simpler, designed to be faster and give the same results.

Table 5.
OpenSkill rating calculation for 2 teams

Player	μ	σ	μ_new	σ_new
Team A (win – ratings go up)				
Player 11	40	2.10	40.12	2.09
Player 12	55	3.30	55.30	3.29
Player 13	35	1.25	35.04	1.25
Player 14	25	6.10	26.01	6.04
Player 15	33	5.92	33.95	5.87
Player 16	25	8.333	26.89	8.18
Team B (loss – ratings go down)				
Player 21	45	1.50	44.94	1.50
Player 22	60	1.30	59.96	1.30
Player 23	30	3.25	29.71	3.24
Player 24	20	5.10	19.29	5.06
Player 25	33	5.92	32.05	5.87
Player 26	25	8.333	23.11	8.19

Table.6.
Comparison of some difference about algorithms

	Win-Lose	**Elo**	**Glicko**	**TrueSkill**	**OpenSkill**
Support for teams	-	+	+	++	++
Fast adaptation for newbie	-	-	+	+	+
Take into account personal performance	-	+	+	++	++
Take into account time when player not in the Game	-	-	+	+ (TrueSkill2)	-
Has control of rank scaling	-	+	+	+	+

Conclusion

In this article, we observed the four popular rating systems for online multiplayer games. We dived into the mathematics behind algorithms and compare the results. It's also clear that every new algorithms is an evolution of the pasts one and that's why all of them have many similarity among each other. And even updates of exist algorithms in some way it is a loan of good idea of other similar algorithms

Elo is the most simple to implement and can easily be good used for PvE games and possible for PvP, but not suitable for multiple teams and asynchronous game modes.

We hope this article has clear up the workings of the most popular rating systems. The focus was on core logic and calculation behind algorithms, so it is not cover all details about them.

References

1.TrueSkill official documentation. URL: https://proceedings.neurips.cc/paper/2006/file/f44ee263952e65b3610b8ba51229d1f9-Paper.pdf
2.TrueSkill2 official documentation. URL: https://www.microsoft.com/en-us/research/uploads/prod/2018/03/trueskill2.pdf
3.Math behind TrueSkill. URL: http://www.moserware.com/assets/computing-your-skill/The%20Math%20Behind%20TrueSkill.pdf
4.Weng Lin official documanteation. URL: https://www.csie.ntu.edu.tw/~cjlin/papers/online_ranking/online_journal.pdf
5.Glicko official documentation. URL: http://www.glicko.net/glicko/glicko.pdf
6.“Developing a generalized Elo rating system for multiplayer games“. URL: https://towardsdatascience.com/developing-a-generalized-elo-rating-system-for-multiplayer-games-b9b495e87802
7.“An ELO based approach to model team players and predict the outcome of games“. URL: https://core.ac.uk/download/pdf/187127715.pdf
8.“The Evaluation of Rating Systems in online free-for-all games” URL: https://arxiv.org/pdf/2008.06787.pdf
9.“Gaussian Process Priors for Dynamic paired comparison modelling”. URL: https://arxiv.org/pdf/1902.07378.pdf/
10. OpenSkill source code. URL: https://github.com/OpenDebates/openskill.py

УДК 004.055, 004.514.2, 004.582

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ІНКЛЮЗИВНОМУ НАВЧАННІ

DOI 10 36994 / 2788- 5518- 2022-02-04-23

Павлик В.Ю. *Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. Vitalik2698@gmail.com*

Самарай В.П., *к.т.н., доц. Відкритий міжнародний університет розвитку людини, Київ, «Україна», Україна. samaraj@ukr.net*

Анотація: *Стаття присвячена аналізу існуючих інформаційно-комунікативних технологій, їх різновидів та можливостей. Проведено огляд нормативно-правових актів, що присвячені інклюзивній освіті та вимогам до організації навчальних процесів з використанням принципів універсального дизайну у навчанні. Пропонуються конкретні варіанти їх застосування у інклюзивному навчанні та варіанти вирішення існуючих проблем з інклюзією.*

Ключові слова: *інклюзія, ІКТ, інформаційно-комунікаційні технології, універсальний дизайн.*

APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN INCLUSIVE EDUCATION

Vitalii Pavlyk. *Open International University of Human Development "Ukraine", Kyiv, Ukraine. Vitalik2698@gmail.com*

Valerii Samarai, *Ph.D.,Ass Prof. Open Internationfl University of Human Development "Ukraine", Kyiv, Ukraine. samaraj@ukr.net*

Abstract: *The article is devoted to the analysis of existing information and communication technologies, their varieties, and possibilities. A review of normative legal acts devoted to inclusive education and requirements for the organization of educational processes using the principles of universal design in education was conducted. This article provides an overview of a number of policy frameworks and international human rights instruments aimed at ensuring equal access to ICT for all, including girls and people with disabilities. Specific options for their application in inclusive education and options for solving existing problems with inclusion are offered. Considered the advantages of inclusive education, the application of the principles of universal design in information and communication technologies, and the universal design of education. The article contains examples of universal learning design. They are organized into eight categories of performance indicators, with general recommendations for each. A set of universal design principles is established to provide guidance in the design of environments, communications, and products that can be applied to academic environments, communications, and products. The main educational components of an inclusive school and the conditions necessary for the optimal use of ICT in inclusive education are defined (School infrastructure, Procurement of good quality equipment, Digital skills, Medical and rehabilitation support, and Coordination to ensure the correct use and maintenance of ICT). Listed the actions needed to increase equitable and effective access to ICT and improve the use of ICT to support inclusive education. The article can be useful for all stakeholders (National governments, Institutional donors, Civil society actors, etc.) in raising the level of inclusive education.*

Key words*: inclusion, ICT, information and communication technology, universal design.*

Вступ

Хоча доступ до освіти покращився з 2000 року, кількість людей, виключених із систем освіти, все ще залишається серйозною проблемою. Кожна одинадцята дитина молодшого шкільного віку позбавлена формальної освіти, причому більшість із них проживає в країнах Африки на південь від Сахари [1]. Соціально-економічний статус і стать дитини є визначальними факторами, але інвалідність є основним фактором виключення [2]. Насправді поєднання кількох факторів посилює освітню відчуженість для мільйонів людей з обмеженими можливостями, чиї численні перешкоди на шляху до освіти часто залишаються поза увагою в освітніх програмах. Крім того, їх перебування у закладі освіти не обов'язково означає, що вони мають ефективний доступ до навчання. Школярі

та студенти з обмеженими можливостями, які відвідують навчальний заклад, часто навчаються в окремих середовищах та/або з ресурсами, які є недостатніми та/або погано адаптованими для забезпечення їхнього успіху в навчанні. Так, люди з обмеженими можливостями в 10 разів рідше відвідують навчальні заклади, ніж інші [3], а діти з обмеженими можливостями в країнах з низьким і середнім рівнем доходів мають на 19% менше шансів отримати базові навички читання, ніж їхні однолітки без обмежень [4].

Виконання досліджень

ІКТ відіграють ключову роль у тому, щоб зробити навчальні заклади місцями отримання знань, навичок і ставлення, вільними від будь-якої форми дискримінації чи сегрегації, надаючи вчителям або лекторам широкий спектр освітнього контенту та заходів, доступних для всіх їхніх учнів. ІКТ можуть допомогти учням подолати труднощі зору, слуху, спілкування, запам'ятовування/концентрації/навчання або руху верхніх кінцівок (це здатність часто потрібна для письма або інших занять).

ІКТ можна розділити на три основні категорії:

• Навчальні матеріали і діяльність, така як: цифрові медіа, метою яких є передача уроків/навичок студенту (наприклад, аудіокнига, навчальне відео з сурдоперекладом тощо).

• Апаратне забезпечення, яке служить посередником для забезпечення доступу до певного навчального контенту/діяльності (наприклад, комп'ютер для перегляду жестового перекладу аудіодокумента).

• Функції доступності, які роблять апаратне забезпечення доступним для всіх (наприклад, програма зчитування екрана, яка дозволяє незрячому студенту або студенту з вадами зору використовувати комп'ютер для доступу до вмісту в Інтернеті).

У рамках міжнародної політики ІКТ вважаються необхідними для створення інклюзивних і справедливих суспільств. Так, низка політичних рамок і міжнародних документів з прав людини спрямовані на забезпечення рівного доступу до ІКТ для всіх, включаючи дівчат та людей з обмеженими можливостями. Зокрема:

• Стаття 9 Конвенції про права людей з інвалідністю вимагає від держав-учасниць сприяти доступу до ІКТ та Інтернету для людей з обмеженими можливостями шляхом заохочення розробки, розробки, виробництва та поширення доступних ІКТ та систем.

• Ціль сталого розвитку (ЦСР 4) закликає до значного розширення доступу до ІКТ та забезпечення загального та зручного доступу до Інтернету в найменш розвинених країнах до 2030 року (ціль 9.c). Вона також спрямована на збільшення використання ІКТ для розширення можливостей жінок за допомогою технологій (ціль 5.b.).

• Загальний коментар Комітету з прав дитини № 25 (2021) щодо прав дітей у цифровому середовищі закликає держави-учасниці просувати технологію, яка відповідає потребам дітей з обмеженими можливостями, і гарантувати, що вона є загальнодоступною, щоб нею могли користуватися всі без винятку діти.

Переваги інклюзивної освіти. Багато досліджень, проведених за останні три десятиліття, показали, що учні з обмеженими можливостями досягають вищих досягнень і покращують навички завдяки інклюзивній освіті, а їхні однолітки без порушень також отримують більшу користь від такого навчання, ніж від звичайного. Для студентів з обмеженими можливостями це включає академічні успіхи в грамотності (читання та письмо), математиці та соціальних науках — як у оцінках, так і на стандартних тестах — кращі комунікативні навички, покращені соціальні навички та більше дружби. Більше часу в загальному класі також пов'язано з меншою кількістю прогулів і покараннями за неприємну поведінку. Це може бути пов'язано з висновками щодо ставлення — вони мають вищу самооцінку, їм більше подобається школа та їхні вчителі, вони більш мотивовані щодо роботи та навчання.

Їх однолітки без інвалідності також виявляють більш позитивне ставлення до тих самих сфер, коли навчаються в інклюзивних класах. Вони досягають більших успіхів у навчанні в читанні та математиці. Дослідження показують, що наявність студентів з обмеженнями дає людям без обмежень нові можливості для навчання. Одна з них – це коли вони виконують роль однолітків. Навчаючись, як допомогти іншому учневі, їхня власна успішність покращується. Інша полягає в

тому, що, коли вчителі більше звертають увагу на своїх різноманітних учнів із обмеженнями, вони надають інструкції з ширшого діапазону методів навчання (візуального, аудіального та кінестетичного), що також приносить користь їхнім звичайним учням.

Часто досліджують проблеми та потенційні “підводні камені”, які можуть зробити навчання менш ефективним у класах інклюзії. Але висновки показують, що це не так. Ані навчальний час, ані кількість залучених учнів між інклюзивними та неінклюзивними класами не відрізняються. Насправді, у багатьох випадках звичайні студенти освітніх закладів повідомляють, що практично не знають про те, що в їхніх класах навіть є студенти з обмеженими можливостями. Коли вони усвідомлюють це, вони демонструють більше сприйняття та толерантності до людей із обмеженнями, коли всі разом отримують інклюзивну освіту.

Застосування принципів універсального дизайну в ІКТ. Універсальний дизайн — це процес створення продуктів, доступних людям із широким діапазоном здібностей, обмежених можливостей та іншими характеристиками. Продукти універсального дизайну враховують індивідуальні переваги та здібності; ефективно передають необхідну інформацію (незалежно від умов навколишнього середовища чи сенсорних можливостей користувача); і до нього можна підійти, досягти, маніпулювати та використовувати незалежно від розміру тіла людини, пози чи рухливості. Застосування принципів універсального дизайну зводить до мінімуму потребу в допоміжних технологіях, створює продукти, сумісні з допоміжними технологіями, і робить продукти зручнішими для всіх, а не лише для людей з обмеженими можливостями.

Як правило, продукти розроблені таким чином, щоб вони були найбільш придатними для середньостатистичного користувача. Навпаки, продукти, розроблені відповідно до принципів універсального дизайну, розроблені таким чином, щоб ними користувався кожен, якомога більше, без потреби в адаптації чи спеціальному дизайні.

Універсальний дизайн зазвичай забезпечує функції продукту, які приносять користь різним користувачам, а не лише людям з обмеженими можливостями. Наприклад, бордюри тротуарів, призначені для того, щоб зробити тротуари та вулиці доступними для тих, хто користується інвалідними візками, сьогодні часто використовують діти на скейтбордах, батьки з дитячими колясками та кур’єри з візками. Так само двері, які автоматично відчиняються, коли хтось наближається до них, є більш доступними для всіх, включаючи маленьких дітей, працівників із повними руками та людей, які користуються ходунками чи інвалідними візками.

Встановлено наступний набір принципів універсального дизайну, щоб забезпечити керівництво в дизайні середовища, комунікацій і продуктів, що можуть бути застосовані до академічного середовища, комунікацій і продуктів:

- Справедливе використання. Цей дизайн корисний і привабливий для людей із різними здібностями. Наприклад, веб-сайт, розроблений таким чином, що він доступний для всіх, у тому числі для незрячих людей, використовує цей принцип.
- Гнучкість у використанні. Конструкція враховує широкий спектр індивідуальних уподобань і можливостей. Прикладом є музей, який дозволяє відвідувачеві читати чи слухати опис вмісту вітрини.
- Просте та інтуїтивно зрозуміле використання. Використання дизайну легко зрозуміти, незалежно від досвіду користувача, знань, мовних навичок або поточного рівня концентрації. Обладнання наукової лабораторії зі зрозумілими та інтуїтивно зрозумілими кнопками керування є хорошим прикладом застосування цього принципу.
- Відчутна інформація. Конструкція ефективно передає необхідну інформацію користувачеві, незалежно від умов навколишнього середовища або сенсорних здібностей користувача. Прикладом використання цього принципу є те, що телевізійні програми, що проектуються в галасливих громадських місцях, як-от експозиції наукових конференцій, включають субтитри.
- Толерантність до помилок. Конструкція мінімізує небезпеки та несприятливі наслідки випадкових або ненавмисних дій. Прикладом продукту, який застосовує цей принцип, є навчальна програма, яка надає вказівки, коли користувач робить невідповідний вибір.
- Низькі фізичні зусилля. Цю конструкцію можна використовувати ефективно, комфортне та з мінімальною втомою. Двері, які легко відкриваються людьми з різними фізичними характеристиками, демонструють застосування цього принципу.

▪ Розмір і простір для підходу та використання. Забезпечується відповідний розмір і простір для підходу, досяжності, маніпуляцій і використання незалежно від розміру тіла, пози чи рухливості користувача. Прикладом використання цього принципу є гнучка робоча зона наукової лабораторії, призначена для використання студентами з різними фізичними характеристиками та здібностями.

Щоб застосувати універсальний дизайн у навчанні, інструктори повинні враховувати можливі варіації в індивідуальних навичках, стилях навчання та вподобаннях, віці, статі, сексуальній орієнтації, культурі, здібностях та обмежених можливостях, коли вони обирають відповідний зміст і стратегії для викладання, а потім застосовують універсальний дизайн до усіх дій та ресурсів курсу.

Принципи що лежать в основі універсального дизайну навчання, можуть бути застосовані до загального дизайну навчання, а також до конкретних навчальних матеріалів, засобів і стратегій (таких як лекції, обговорення в класі, групова робота, веб-інструкції, лабораторні роботи, польові роботи та демонстрації). Нижче наведено приклади універсального дизайну навчання. Вони організовані за вісьмома категоріями показників ефективності, із загальними рекомендаціями для кожної:

- Цінності класу. Приймайте методи, які відображають високі цінності щодо різноманітності, справедливості та залучення. Приклад: розмістить заяву у своєму навчальному плані, запрошуючи студентів зустрітися з вами, щоб обговорити пристосування, пов’язані з інвалідністю, та інші особливі навчальні потреби.
- Взаємодія. Заохочуйте регулярну та ефективну взаємодію між учнями, використовуйте різноманітні методи спілкування та переконайтеся, що методи спілкування доступні для всіх учасників. Приклад: призначте групову роботу, до якої учні повинні брати участь, використовуючи різні навички та ролі.
- Фізичні середовища та продукти. Для зовнішнього навчання переконайтеся, що об’єкти, види діяльності, матеріали та обладнання фізично доступні для всіх студентів, а також що з точки зору безпеки враховуються різноманітні потенційні характеристики студентів. Приклад: розробіть процедури безпеки для всіх студентів, у тому числі для сліпих, глухих або користувачів інвалідних візків.
- Способи доставки. Використовуйте кілька методів навчання, які доступні всім учням. Приклад: використовуйте кілька режимів для доставки вмісту; коли це можливо, дозвольте учням вибирати з кількох варіантів навчання; а також мотивуйте та залучайте студентів — розгляньте лекції, варіанти спільного навчання, практичні заняття, спілкування через Інтернет, освітнє програмне забезпечення, польову роботу тощо.
- Інформаційні ресурси та технології. Переконайтеся, що навчальні матеріали, примітки та інші інформаційні ресурси є привабливими, гнучкими та доступними для всіх студентів. Приклад: виберіть друковані матеріали та підготуйте програму завчасно, щоб дати студентам можливість почати читати матеріали та працювати над завданнями до початку курсу. Дайте достатньо часу, щоб організувати альтернативні формати, наприклад книги в аудіоформаті.
- Зворотній зв'язок і оцінка. Регулярно оцінюйте прогрес студентів, регулярно надавайте конкретні відгуки, використовуючи численні доступні методи та інструменти, і відповідно коригуйте інструкції. Приклад: дозвольте учням здавати частини великих проектів для отримання відгуків до того, як настане остаточний проект.
- Розміщення. План розміщення студентів, чиї потреби не повністю задовольняються змістом навчання та практикою. Приклад: знайте протоколи кампусу для отримання матеріалів в альтернативних форматах, перепланування класних кімнат і організації інших приміщень для студентів з обмеженими можливостями.

Остання класифікація практик універсального дизайну навчання є важливою, оскільки використання його принципів не усуває потреби в спеціальних пристосуваннях для студентів з обмеженими можливостями. Наприклад, вам може знадобитися надати сурдоперекладача глухому студенту. Однак застосування концепцій універсального дизайну навчання при плануванні курсу забезпечує повний доступ до контенту для більшості студентів і мінімізує потребу в спеціальних пристосуваннях. Наприклад, створення веб-ресурсів у доступних форматах у міру їх розробки означає відсутність перепланування, необхідного, якщо до класу зараховується

незрячий учень.

Універсальний дизайн навчання приносить користь студентам з обмеженими можливостями, але також приносить користь іншим. Наприклад, субтитри до відеороликів курсу, які надають доступ глухим або слабочуючим студентам, також є перевагою для студентів, для яких українська є другою мовою, для деяких студентів із вадами навчання та для тих, хто дивиться стрічку в шумному оточенні. Надлишкове надання вмісту може покращити навчання для студентів із різними стилями навчання та культурним походженням. Надання всім учням доступу до ваших нотаток і завдань на веб-сайті принесе користь як студентам з обмеженими можливостями, так і всім іншим. Планування наперед економить час у довгостроковій перспективі.

ІКТ для підтримки інклюзивної освіти

Системи інклюзивної освіти спрямовані на задоволення різноманітних потреб усіх дітей та молоді, щоб вони могли навчатися, рости та розвиватися разом.

Основні освітні компоненти інклюзивної школи:

- Спілкування з учителем або лектором;
- Спілкування з учнями;
- Доступ до письмового матеріалу (підручники, інформація, написана на дошці тощо);
- Доступ до усного матеріалу (аудіоматеріали, тощо);
- Можливість висловлюватися письмово (здати письмове домашнє завдання; скласти письмовий іспит тощо);
- Можливість висловлюватися усно (зробити презентації/подати усні домашні завдання, скласти усні іспити тощо);
- Можливість робити нотатки;
- Отримання доступу до різних педагогічних інструментів/навчальних матеріалів, що пропонуються (навчання ІТ-навички, перегляд відео тощо).

Умови, необхідні для оптимального використання ІКТ в інклюзивній освіті. В більшості випадків для оптимального використання ІКТ в інклюзивній освіті необхідно виконати низку умов [6]. У країнах із низьким і середнім рівнем доходу вже є багато прикладів значного прогресу у досягненні цих умов, і вони підтверджують життєво важливе значення встановлення партнерства та координації між ключовими гравцями (включно з урядами, приватним сектором, інституційними донорами, агентствами ООН, школами та університети) і пошуку інноваційних рішень.

Умова 1: Інфраструктура навчального закладу.

Для більшості ІКТ потрібен доступ до електроенергії для зарядки або використання. Багато шкіл, особливо в сільській місцевості, не підключені до електромережі або мають обмежений доступ до якісної електроенергії (тобто електроенергії, яка не пошкоджує обладнання). В Україні дана проблема особливо актуальна після ракетних обстрілів енергетики ворогом - у всіх регіонах України «Укренерго» застосовує аварійні відключення світла через стрімке зростання дефіциту потужності. Причиною збільшення дефіциту потужності стали непрогнозовані аварійні відключення блоків на кількох електростанціях. Крім того, споживання електроенергії зростає через погіршення погодних умов. У країнах Африки ситуація також складна і без аварійних відключень. Так, у Беніні лише 42% населення має доступ до електроенергії, а на Мадагаскарі – 26% [7]. Деякі ІКТ (особливо більш просунуті інструменти) також вимагають підключення до Інтернету, але в більшості країн з низьким рівнем доходу фіксований Інтернет все ще дуже обмежений, а мобільний Інтернет занадто дорогий. Наприклад, у Буркіна-Фасо лише 16% населення користується фіксованим Інтернетом [8], але 65% населення охоплено 3G [9]. В Україні ситуація зараз також дестабілізована через проблеми зі сторони провайдерів.

Умова 2: Закупівля якісного обладнання.

Вартість є однією з основних перешкод для використання ІКТ у навчальних закладах. Комерційно доступне зчитування з екрана або програмне забезпечення для створення символів може реально змінити життя учнів з обмеженими можливостями, але часто це надто дорого [10]. Крім того, деякі ІКТ, виявлені в навчальних закладах різних країн не відповідають потребам учнів і, нарешті, доступність ІКТ місцевими мовами є надзвичайно рідкою.

Умова 3: цифрові навички.

Більшість учителів, учнів і батьків у цільових країнах дослідження дуже мало стикалися з ІКТ і мають дуже мало цифрових навичок. Це головна перешкода для використання ІКТ у класі та для дистанційного навчання. Певний рівень грамотності також є важливою передумовою для того, щоб навчитися користуватися певними ІКТ. Через низький рівень грамотності серед членів родини чи опікунів домашня підтримка, яку можна надати цим дітям у навчанні та розвитку необхідних цифрових навичок, обмежена.

Умова 4: Медична та реабілітаційна підтримка.

Визначення необхідних послуг та інструментів вимагає підтримки міждисциплінарної команди. Обмежений доступ до спеціалістів із охорони здоров'я та реабілітації (фізіотерапевтів, ерготерапевтів, логопедів тощо) залишається перешкодою для діагностики інвалідності та визначення типу ІКТ, які відповідають потребам дитини, а також для здійснення необхідних адаптацій до будинку дитини. і шкільне середовище (наприклад, через планування простору та меблі, адаптовані для використання ІКТ).

Умова 5: Координація для забезпечення правильного використання та підтримки ІКТ.

Необхідне узгодження ІКТ та етики в інклюзивній освіті. Наприклад, за допомогою деяких засобів ІКТ діти, які використовують їх для виконання вправ, відокремлені від решти класу. Тому дуже важливо розглянути етичні питання за участю перед впровадженням освітньої програми, яка передбачає використання засобів ІКТ.

Варіанти вирішення існуючих проблем. Перелік дій, необхідних для збільшення справедливого та ефективного доступу до ІКТ та покращення використання ІКТ на підтримку інклюзивної освіти:

Національним урядам бажано:

- ІНТЕГРУВАТИ ІКТ у свої плани в галузі освіти і існуючі та майбутні освітні стратегії, а також виділення конкретних бюджетів для їх реалізації. Оскільки уряди переглядають свої бюджети після COVID-19, інвестиції в інклюзивну освіту є життєво важливими, щоб діти з обмеженими можливостями більше не залишалися осторонь:

1) Надати пріоритет у своїх проектах розвитку інфраструктури підключенню шкіл до електроенергії та Інтернету.

2) Забезпечити цифрове навчання для вчителів, батьків, опікунів і учнів, приділяючи особливу увагу дітям з обмеженими можливостями. Для вчителів цей тренінг має включати модулі з використання ІКТ та базових налаштувань і керування обслуговуванням.

3) Шукати офіційні угоди з постачальниками (виробники комп'ютерів/планшетів/телефонів, розробники програмного забезпечення, оператори мобільного зв'язку, технологічні сервісні компанії тощо), особливо на місцевому рівні, щоб знайти рішення для збереження вартості ІКТ на доступному рівні та підтримки вільного доступу до підключення або електрики у певних виняткових умовах (наприклад, для дистанційного навчання під час великої кризи).

- ЗАБЕЗПЕЧИТИ, щоб Міністерство освіти систематично наділялося повноваженнями очолити співпрацю з іншими міністерствами та секторами шляхом створення та підтримки багатосторонніх платформ (представників шкіл, неурядових організацій, залучених міжнародних організацій, приватного сектора тощо) та багатогалузевих платформ (освіта, охорона здоров'я, реабілітація, інфраструктура, технології, енергетика, гендерна рівність).
- ВИКОРИСТОВУВАТИ будь-які можливості, щоб інтегрувати використання ІКТ в освіті в свої політичні плани цифровізації, розвитку інфраструктури та соціальної інтеграції.

Інституційним донорам бажано:

- ВІДДАВАТИ ПРІОРИТЕТ інклюзивній освіті в програмах допомоги, особливо у відповідь на пандемію та воєнні дії, враховуючи їх катастрофічний вплив на доступ до освіти для дітей з обмеженими можливостями.
- ЗБІЛЬШИТИ фінансування для підтримки трансформації до інклюзивних, якісних систем освіти, які максимізують потенціал інструментів ІКТ для сприяння залученню дітей з обмеженими можливостями та маргіналізованих учнів.

• ІНВЕСТУВАТИ та підтримувати інновації, дослідження та розробку доступних і доступних ІКТ для вирішення проблем інклюзивної освіти, включаючи дистанційну та/або онлайн-навчання.

Учасникам громадянського суспільства (організації людей з обмеженими можливостями, НУО, місцеві асоціації тощо) бажано:

• СПРИЯТИ партнерству та ПІДВИЩИТИ ОБІЗНАНІСТЬ серед зацікавлених сторін, особливо урядів, сприяючи діалогу, обмінюючись відповідними ресурсами та даними про освітню ситуацію дітей з обмеженими можливостями та потенціал ІКТ, а також підтримуючи зусилля з переходу до більш інклюзивних систем освіти. Основним глобальним технологічним гравцям треба підкреслювати ключову роль у забезпеченні доступності своїх продуктів для максимальної кількості людей через застосування принципів універсального дизайну, особливо в країнах з низьким і середнім рівнем доходу. З цією метою слід посилатися на Марракешську угоду [11], що полегшує виробництво та міжнародну передачу книг, спеціально адаптованих для сліпих або людей із вадами зору, встановлюючи набір обмежень і винятків із традиційного авторського права.

Усім зацікавленим сторонам бажано:

- ВИЗНАЧАТИ передові практики, підтримувати їх впровадження та сприяти їх повторюваності для оптимального та ширшого використання ІКТ у навчанні на підтримку більш інклюзивної освіти.
- ЗАБЕЗПЕЧИТИ суттєву участь зацікавлених людей (осіб з обмеженими можливостями, дітей, батьків, вчителів) та організацій, що їх представляють, на всіх етапах впровадження інклюзивних освітніх програм, у тому числі щодо використання ІКТ.
- ПРИЙНЯТИ гендерно-чутливий підхід шляхом усунення відмінностей у доступі до підключення та цифрового навчання та сприяння можливостям застосування цих навичок на практиці.
- ЗБИРАТИ, аналізувати та обмінюватися даними про освітню відчуженість, навчальні потреби та доступ до ІКТ, дезагреговані за віком, статтю та інвалідністю.

Висновки

Інформаційно-комунікаційні технології відіграють важливу роль в інклюзивному навчанні школярів та студентів. Для покращення стану інклюзивної освіти та її забезпечення більшій кількості людей, урядам варто інтегрувати ІКТ у свої плани в галузі освіти і існуючі та майбутні освітні стратегії, а також виділити конкретні бюджети для їх реалізації. Учасникам громадянського суспільства (організації людей з обмеженими можливостями, НУО, місцеві асоціації тощо) слід сприяти партнерству та підвищенню обізнаності серед зацікавлених сторін, а зацікавленим сторонам варто визначити передові практики, підтримувати їх впровадження та сприяти їх повторюваності для оптимального та ширшого використання ІКТ у навчанні на підтримку більш інклюзивної освіти.

References

1. UNESCO-UIS (2018). Fact Sheet N¬∞48: Кожна п'ята дитина, підліток і молодь не відвідує школу.
2. UNICEF (2021). Боротьба з втратою ізоляції для дітей з обмеженими можливостями та їхніх сімей.
3. Plan International (2019). План міжнародної агітації. URL: https://www.plan-international.fr/news/2019-12-03-plan-international-agit-pour-leducation-des-enfants-handicapes
4. UNESCO (2020). Global Education Monitoring Report.
5. The study " Barriers and levers for the use of telerehabilitation through experimentation in three countries ", also conducted by Humanity & Inclusion, outlines similar barriers to be lifted and conditions to be in place (training of professionals, sustainable economic model, increased ICT skills, robust policy framework, and collaboration among stakeholders).
6. The study « Barriers and levers for the use of telerehabilitation through experimentation in three countries », also conducted by Human- ity & Inclusion, outlines similar barriers to be lifted and conditions to be in place (training of professionals, sustainable economic model, increased ICT skills, robust policy framework, and collaboration among stakeholders). .
7. GSMA Intelligence, прогнози 2020.
8. The Education Commission (2016). Як технології можуть змінити правила інклюзивної освіти.

9. The Marrakesh Treaty was adopted on 27 June 2013 in Marrakesh and forms part of the international copyright treaties administered by WIPO.
10. professionals, sustainable economic model, increased ICT skills, robust policy framework, and collaboration among stakeholders).
11. World Bank (2018).
12. World Bank (2017).
13. GSMA Intelligence,2020 forecasts.
14. The Education Commission (2016). How technology can be a game changer for inclusive education.
15. The Marrakesh Treaty was adopted on 27 June 2013 in Marrakesh and forms part of the international copyright

УДК 004.7, 004.75, 004,85

ОГЛЯД АКТУАЛЬНИХ ШЛЯХІВ ПРИСКОРЕННЯ РОБОТИ З НАВЧАЛЬНИМИ ДАНИМИ У СИСТЕМАХ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ МОВЛЕННЯ

DOI 10 36994 / 2788- 5518- 2022-02-04-24

Шульга Ю.А. *Відкритий міжнародний університет розвитку людини «Україна»,Київ,Україна. yuhim1308@gmail.com*

Забара С.С., *д.т.н., проф..Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. staszabara@gmail.com*

Анотація: *В умовах збільшення кількості голосових зразків для обробки основним завданням є пришвидшення роботи із навчальними даними та збереження швидкодії та відмовостійкості систем розпізнавання вцілому, що стає доступним при використанні розподілених та децентралізованих систем. Використання багатохмарних підходів дозволяє отримувати переваги від використання кожної з них та отримуючи масштабованість, більшу кількість обчислень за одиницю часу та зменшення часу очікування на результат.*

Ключові слова: *розпізнавання мовлення, розподілені системи, децентралізовані системи, глибинне навчання.*

REVIEW OF CURRENT WAYS OF ACCELERATING WORK WITH TRAINING DATA IN AUTOMATIC SPEECH RECOGNITION SYSTEMS

Yukhym Shulha. *Open International University of Human Development "Ukraine", Kyiv, Ukraine. yuhim1308@gmail.com*

Stanislav Zabara, *Dr.habil., Prof. Open International University of Human Development "Ukraine", Kyiv, Ukraine. staszabara@gmail.com*

Abstract: *The training data and preserve the speed and fault tolerance of recognition systems as a whole, which becomes available when using distributed and decentralized systems. To process a large number of requests, it is necessary to keep the initial database up-to-date, taking into account trends in system usage and received new or abnormal requests. For the development of such systems, both logical or topological and algorithmic approaches are used. Each of them has its own shortcomings and advantages, which need to be studied for use in each system to obtain optimal results. The use of multi-cloud approaches allows you to get the benefits of using each of them and getting scalability, a greater number of calculations per unit of time, and a reduction in waiting time for the result. For a preliminary analysis of features and potential complex architectural solutions when working with state-of-the-art approaches, already existing studies were reviewed to identify the necessary improvements and the possibility of application in a wide range of systems. The combination of acceleration and availability is one of the most important because the use of the most modern algorithms may require the use of specific hardware. Extensive research uses specialized equipment of the same type connected by a high-bandwidth local network, which in practical designs will require the use of a multidimensional architectural approach, which will require a balanced use of the geographical location of computing centers in order to reduce delays between system elements to balance the obtained acceleration and potentially possible delays in the transmission of information between elements located in different treatment centers.*

Key words: *speech recognition, distributed systems, deep learning.*

Вступ

Розвиток система автоматичного розпізнавання в умовах збільшення кількості голосових зразків вимагає адаптації процесу розпізнавання для зберігання автентичних та оброблених голосових записів. Децентралізація та розподілення є одними із найкращих способів забезпечення

не тільки для збереження автентичності й недопущення підміни голосових зразків, а ще і для прискорення роботи системи вцілому. Важливо створити умови для ефективного розподіленого навчання, а також щоби алгоритми навчання могли збігатися з великим розміром пакета. Стратегія розвитку систем такого роду має містити декілька основних етапів. Перший етап повинен дослідити основні гіперпараметри (напр. швидкість навчання, об'єм навчальної бази) це необхідно для забезпечення належної точності, використовуючи, у роботі пакети різних розмірів. Наступний етап більш практичний і потребує практичного тестування стратегій (синхронну, асинхронну, асинхронну децентралізовану паралельну стохастичного градієнтного спуску й гібридну). Під час роботи з децентралізованими системами розпізнавання мовлення експерименти показали, що використання асинхронного децентралізованого паралельного стохастичного градієнтного спуску дає можливість працювати з розміром пакету, що втричі більший за розмір пакету для синхронного стохастичного градієнтного спуску. Дослідження показують, що цей розвиток досить перспективний і показує добру масштабованість і суттєве пришвидшення роботи моделі, однак таке прискорення можливе в разі використання однотипного спеціалізованого обладнання, що, може, накласти певні обмеження на практичне використання таких методів. Нівелюють таку потребу потенційно набагато продуктивніші квантові обчислювальні кластери, а також модульний підхід до створення обчислювального кластеру, який, може, бути легко масштабований шляхом залучення нових обчислювальнихх клієнтів, на які, може, бути розподілені задачі з обчислення. Хоча останній підхід не є повністю децентралізованим, а розподіленим його можна зробити децентралізованим, використовуючи, блокчейн підхід у розробленні.

Виконання досліджень

Системи автоматичного розпізнавання мовлення з моменту своєї появи демонстрували суттєвий та стабільне зростання та впровадження у велику кількість галузей. Особливо привабливі системи автоматичного розпізнавання стали після початку їх доступності у форматі ПЗ, як сервіс, а в часи пандемії ріст впровадження систем автоматичного розпізнавання мовлення склав 23 %. Розпізнавання мовлення — це одна з перших галузей, де методи глибинного навчання дають змогу одержувати суттєво кращі результати за менший термін необхідний для виконання. Для того, аби отримати репрезентативні результати важливо комбінувати підходи та стратегії роботи із системами автоматичного розпізнавання мовлення для забезпечення необхідної продуктивності. Найвагомішим елементом, що забезпечує продуктивну роботу системи є навчальні дані. Обсяг тренувальних даних для систем розпізнавання мовлення для типових задач складає від тисячі до десятків тисяч годин, а вузькоспеціалізовані задачі використовують до мільйона годин. Такий великий об'єм даних потрібно результативно та безпечно обробити. Обробка такого масиву даних на одному обчислювальному елементі, може, зайняти роки тож логічним кроком є застосування підходів, за допомогою, яких час на обробку скоротиться. Підходи розподіляються на алгоритмічні та структурні. Найчастішим та ефективним підходом є розподілене навчання. Розподілене навчання широко використовується у сферах машинного зору, адже має подібні до систем автоматичного розпізнавання мовлення алгоритмічні та структурні схеми. Це важливе уточнення адже ці сфери мають подібну структуру тому схеми пришвидшення роботи не завжди суміжні, а найчастіше не взаємозамінні, тобто, пряме запозичення технік, може, не дати бажаного результату.

Логічні підходи розподіляються відповідно до топології. їх є три: централізована, кооперативна й некооперативна (рис.1).

Централізована топологія містить у собі центр обробки або ж злиття даних, що виконує задачі з отримання даних, розподілу завдань та збору результатів. Завдяки наявності в структурі такого центру прямого спілкування між агентами не відбувається, що робить таку схему досить простою, розповсюдженою та досить просто масштабованою. Однак наявність централізованого вузла керування вносить у систему вразливість та створює вузьке місце в пропускній здатності системи, що й доводять дослідження різних груп дослідників. Але зважаючи на широку розповсюдженість розроблені практичні підходи, які дають змогу максимально нівелювати негативні впливи. Однак для роботи із розподіленим, а тим паче із децентралізованими підходами ця схема не може бути застосована. Через це для оптимізації систем застосовують кооперативна й некооперативна. У

некооперативній топології всі агенти незалежні один від одного, що дозволяє їм реалізувати власні очікування. Кожен агент самостійно ділиться даними та своєю поведінкою. А в кооперативній кожен з агентів має додатковий зв'язок, що дозволяє отримувати більше інформації про завдання та стани в програмному вигляді реалізований у вигляді балансувального алгоритму для кращого розподілу завдань. Крім, того, у такий спосіб збільшується стійкість до несправностей та відмов, збільшити конфіденційність даних, збільшити потужність розподіленої обробки інформації в мережі.

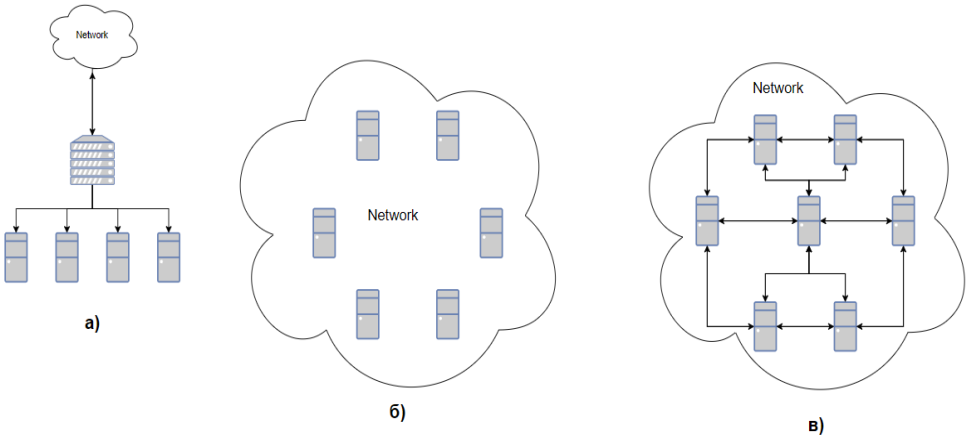


Рис.1. Різновид топологій: а) Централізована; б) Децентралізована не кооперативна; в) Децентралізована кооперативна

Структурні підходи містять у собі логічні підходи, однак, спрямовані на впровадження в практичну реалізацію для отримання найкращих показників. Усі структурні стратегії, що можуть бути застосовані до систем автоматичного розпізнавання можна виокремити в такі групи :

- *Паралельний доступ до даних* та *паралельне підключення до моделі*:

Паралелізм даних розподіляє мініпакети даних між кількома учнями (наприклад, GPU або CPU), причому кожен учень має копію моделі. Обчислення виконується для кожного учня паралельно з використанням даних перед тим, як система певним чином агрегує статистичні дані. Іноді модель занадто велика, щоби поміститися в пам'ять одного учня. За цієї умови паралелізм моделі використовується для розподілу моделі між учнями водночас кожен учень має, лише часткову модель. Вихідні дані одного учня використовуються, як вхідні дані іншого учня для проведення обчислень повної моделі. Хоча паралелізм моделей використовується в деяких сценаріях, паралелізм даних є домінуючою розподіленою стратегією на практиці в сучасній спільноті розподіленого навчання.

- *Одно вузлова* та *багато вузлова структура*:

Під вузлом розуміється фізичний пристрій (наприклад, сервер) у комп'ютерній мережі. Розподілене навчання на одному вузлі — це коли всі учні (наприклад, графічні процесори) залишаються на одній машині зі спільною пам'яттю. Спілкування між учнями є надійним і, може, забезпечити помірне прискорення. Тобто такий варіант усе ще розумний підхід для розподіленого навчання нейронних мереж. Очевидно, що він має обмеження щодо можливості масштабування, а кількість учнів обмежена апаратною конфігурацією машин. Розподілене навчання з декількома вузлами має кілька машин (вузлів) для формування хмари або кластера, де учні використовують спільну пам'ять для локального зв'язку всередині вузла та передачу повідомлень через мережу для зв'язку між вузлами. Це стало нормою для останніх масштабних розподілених тренувань.

- *Централізоване* та *децентралізоване навчання*:

Централізоване розподілене навчання покладається на центральний вузол, і всі учні спілкуються з центральним вузлом, лише для оновлення моделі та передачі результатів. Децентралізоване налаштування не має центрального вузла, і всі учні утворюють мережу певної топології (наприклад, кільце). Усі учні перебувають у рівному становищі щодо обчислень і

спілкування. Централізоване розподілене навчання зазвичай використовується на практиці в багатьох програмах машинного навчання. Однак це створює велике вузьке місце у вигляді центрального вузла, коли кількість учнів велика. З іншого боку, децентралізоване розподілене навчання має перевагу в пропускній здатності зв'язку та стає все більш популярним, хоча і проєктування та адаптація системи займає набагато більше ресурсів.

- *Синхронне* та *асинхронне навчання*:

Алгоритми розподіленого навчання можуть працювати в синхронному або асинхронному режимі. У синхронному режимі обчислення та оновлення моделі синхронізуються одне з одним. Оновлення моделі виконується після того, як усі учні завершать обчислення локального завдання. Однак в асинхронному режимі синхронізація між обчисленням і оновленням моделі видаляється, й учні отримують свої мініпакети за потреби залежно від статусу своїх обчислень і швидкості зв'язку, що значно скорочує час простою, порівнюючи, із синхронним режимом.

З практичної точки зору створення повністю децентралізованої системи вимагає значних зусиль, а певні процеси, що притаманні роботі зі звуковими сигналами повноцінно децентралізувати неможливо тому найоптимальнішим є використання розподілених систем. Основні зусилля такої системи спрямовані на розподіл процесу розпізнавання на процеси за можливістю паралельного виконання. У кінцевому результаті, виходить, система, що складається з таких частин:

- Паралельна частина, яка, може, виконуватися паралельно, наприклад, градієнтне обчислення.
- Послідовна частина, яку не можна розпаралелити. Наприклад, підсумовування градієнтів або моделей, може, бути виконано, лише після того, як градієнти або моделі будуть на місці.
- Комунікаційна частина, яка передає інформацію між обчислювальними ресурсами, наприклад, передача градієнта/ваги між учнями.

Для оцінювання потенційного прискорення такої системи використовують закон Амдала застосований до найбільш використовуваного алгоритму при розподіленому навчанні, а саме стохастичного градієнтного спуску(англ. Stochastic gradient descent, SGD). Припускаючи, що вартість зв'язку дорівнює нулю, то згідно з законом Амдала прискорення паралельної програми обмежене$\frac{1}{1-p}$, де p є частиною розпаралелюваної частини програми. Для алгоритму SGD паралельна частина домінує над послідовною. Отже, p дуже близьке до 1, і в принципі можна досягти дуже високих прискорень. Як наслідок, основним обмежуючим чинником для досягнення лінійного прискорення в цьому випадку є вартість зв'язку.

Типова система розподіленого навчання, як зображено на рис. 1, має такі апаратні компоненти (рис.2):

- сховище даних
- пам'ять, процесори (CPU/GPU)
- мережу.

Передача даних відбувається за такий спосіб: кожен учень завантажує вхідні дані зі сховища даних з обмеженням пропускної здатності сховища в основну пам'ять. Він проводить попередню обробку даних із допомогою центрального процесора перед тим, як відправити їх на графічний процесор через шину передачі даних для навчання моделі. Коли обчислення градієнта завершено, градієнти надсилаються до центрального процесора або іншим учням згідно з обмеженням пропускної здатності мережі. Типова пропускна здатність систем зберігання коливається залежно від типу

- 1–10 МБ/с (мережева файлова система) до 100 МБ/с (жорсткі диски, HDD),
- 300–500 МБ/с (твердотільний накопичувач, SSD), до кількох ГБ/с (SSD з енергонезалежною пам'яттю Express (NVMe)).
- Типова пропускна здатність основної пам'яті становить кілька десятків ГБ/с.
- Типова пропускна здатність шини даних CPU-GPU коливається від 16 ГБ/с в одну сторону (наприклад, PCI-e 3-го покоління) до 50 ГБ/с в одну сторону (наприклад, IBM Power 9 Nvlink).

- Типова пропускна здатність мережі коливається від 100 МБ/с (наприклад, 1 Гбіт Ethernet) до 10 ГБ/с (наприклад, 100 Гбіт Ethernet, RDMA).

Кластер HPC високого класу (наприклад, суперкомп’ютер SUMMIT) зазвичай оснащений NVMe SSD, NVlinks і 100Gb Ethernet (або вище) для забезпечення швидкого зв’язку. З боку обчислень ключовим вирішальним чинником є FLOPS (англ. Floating Point Operations Per Second, FLOPS), Типові процесори високого класу працюють зі швидкістю від сотень FLOPS до 1 FLOPS, а типові процесори високого класу

Графічні процесори працюють на 10 TFLOPS або вище. Системні програмісти використовують паралельне програмування, яке зазвичай досягається з допомогою багатопоточності, щоби перекривати зв’язок з обчисленнями. У синхронному режимі,завантаження та обробка даних можуть накладатися на градієнтне обчислення. В асинхронному режимі всі шляхи зв’язку (тобто завантаження даних, попередня обробка даних, передача даних CPU-GPU і передача градієнтів/ваг) можуть перекриватися градієнтними обчисленнями. У такі спроби покращення мають на меті досягти ідеального перекриття між комунікацією та обчисленнями. На практиці спілкування, які не можуть бути перекриті обчисленнями, є обмежуючим чинником у досягненні лінійного прискорення. Одним із важливих завдань у розробленні розподіленого навчання є максимізація перекриття між ними.

Для розподіленого навчання використовують алгоритм градієнтного спуск та різні його варіації, а саме градієнтний спуск, синхронний градієнтний спуск, асинхронний градієнтний спуск та гібридний варіант градієнтного спуску, а також різні набори навчальних даних. Аналізуючи дослідження можна зробити висновок, що для роботи із розподіленими системами оптимальним вибором буде асинхронний децентралізований паралельний стохастичний градієнтний спуск (рис.3). Експерименти з алгоритмами навчання дають змогу виявити вузькі місця системи адже менша кількість навчальних даних не дозволить навчити систему так, щоби виявити вузьке місце, а більший дозволить пристосувати роботу до вузьких місць, а інша алгоритмічна структура не буде використовувати апаратну частину системи в об’ємах достатніх для виявлення проблем та вираховування потенційного приросту. Станом на зараз у літературі є ґрунтовні дослідження, які використовують асинхронний децентралізований паралельний стохастичний градієнтний спуск та показують суттєвий приріст швидкодії за умови використання градієнтного спуску.

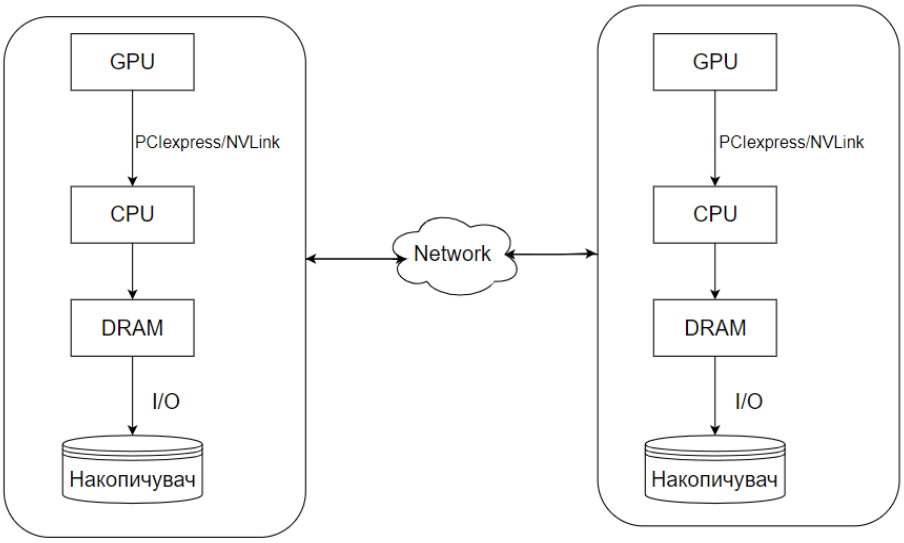


Рис.2. Компоненти та потоки даних у високопродуктивному обчислювальному середовищі для розподіл еного навчання

Варто зазначити, що дослідження проводилися на спеціальному обладнанні, що не потребує додаткових операцій із пристосування до роботи з обладнанням, а цей чинник позитивно впливає, як на швидкодію так і на точність результатів. У дослідженнях використовувалися навчальні бази

тривалістю до 2000 годин та 128 графічних ядер Nvidia V100. Результати досліджень показують результати прискорень до 50 раз (табл.1), однак у такому варіанті важливо забезпечити високу швидкодію між елементами адже відставання доставки пакету до одного із компонентів означатиме не повне або ж взагалі неможливе виконання операції (табл.1).

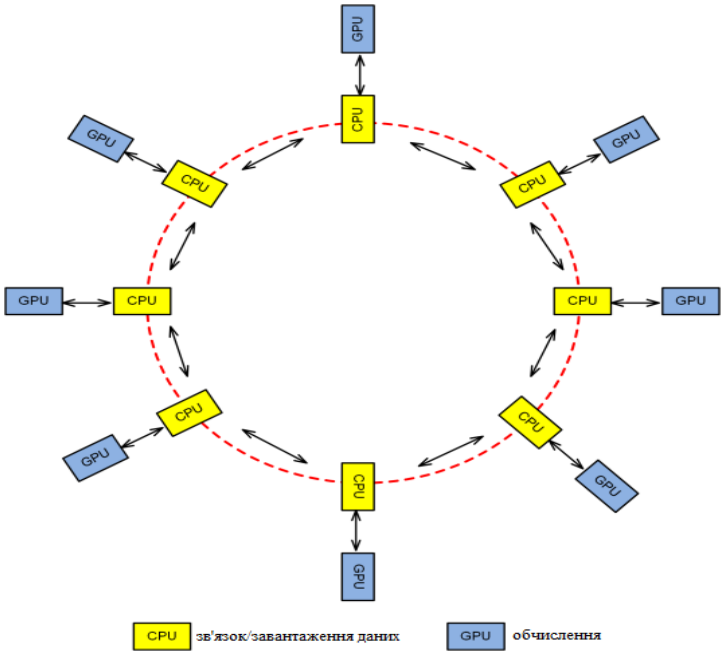


Рис.3. Ілюстрація впровадження ADPSGD, усі учні утворюють кільце

Кожен учень має обчислення локального градієнта, що виконується на графічному процесорі, усереднення моделі з іншими учнями та завантаження даних на центральний процесор. Два процеси здійснюються одночасно.

Для побудови практичних систем у перелічених дослідницьких роботах цікавлять показники: час прискорення та показник помилок на слово. Ці показники цікавлять через прямий вплив на побудову архітектури системи вцілому адже час прискорення показує, скільки потенційно часу можна одержати для виконання інших операцій (рис.4) та дати прискорення в роботі кінцевому користувачу також важливий цей показник тим, що в разі виникнення несправностей дасть змогу перевести на роботу на резервний елемент системи (в разі наявності такого) або ж відновити роботу в штатному режимі та дати користувачу результат виконання, а показник помилок на слово показник важливий тим, що саме його мінімальне значення дає змогу відрізків, тож кінцевий користувач одержить бажаний результат без тривалого очікування та небажаного спотворення аудіозапису. Ці дослідження показують певні особливості проєктування систем розпізнавання. Під час впровадженні таких обчислювальних елементів у гібридну або ж багатохмарну інфраструктурну схему варто враховувати необхідність забезпечення каналів комунікації з високою швидкодією для отримання прискорення від використання таких обчислювальних елементів. Потрібно звернути увагу на критичну необхідність резервування, як мережевих з’єднань так і всіх елементів системи адже стійкість системи до поломок дасть змогу гарантовано одержувати бажані результати.

К-ть учнів	Розмір пакету	Загальний розмір	WER%		Час (год)	Прискорення
			SWB	CH		
1	128	128	7,5	13,0	121,96	
1	256	256	7,5	13,0	99,0	1.0x
1	512	512	7,5	13,1	82,06	1.2x
16	512	8,192	7,4	13,3	5,88	16.8x
32	256	8,192	7,6	13,1	3,60	27.5x
64	128	8,192	7,5	13,3	2,28	43.4x
128	64	8,192	7,7	13,3	1,98	50.x

Для більш повного розуміння прискорення потрібно проаналізувати і втрати, які можуть виникати під час роботи із даними. Як було зазначення для максимального прискорення втрати мусять бути відсутні або ж мінімальні. Стійкість до втрат важливий параметр адже в реальних умовах повна відсутність втрат, може, вимагати складних архітектурних рішень. Для порівняння втрат ADPSGD під час роботи з даними в дослідженнях використовують SSGD тобто синхронний стохастичний градієнтний спуск .Таке порівняння показує перевагу асинхронного виконання перед синхронним у швидкості, адже в разі використання SSGD учні обчислюють градієнт і чекають, поки буде обчислено всі градієнти, потім модель оновлюється та знову розповсюджується всім учням, чого не відбувається в асинхронному режимі адже кожен учень отримує новий градієнт після завершення обчислення, але синхронний варіант має більшу лояльність до втрат, хоча й поступається в прискоренні .

Також маю зазначити, що ці вищезгадані дослідження доводять раціональність використання платформних підходів під час розробки чи проєктування систем розпізнавання, що забезпечуватиме масштабованість і адаптивність та позитивно впливатиме на безпеці. Такі варіанти обчислювальних систем уже реалізовані практично, основна особливість їх є не використання спеціальних обчислювальних нод, а створення таких, використовуючи, певну кількісті обчислювальних елементів об’єднаних в одну ноду, що сумарно дають таку ж обчислювальну потужність, що й системи, які використовувались у дослідженнях. У такому підході основними плюсами є суттєво нижчий рівень вартості та простота в масштабуванні, однак, основними питанням є забезпечення швидкодії між елементами та час виконання операції. У разі роботи з простою обробкою попередньо збереженої навчальної бази теоретично можна знехтувати незначним збільшенням часу на виконання з огляду на меншу вартість. Однак робота в режимі реального часу або ж із великими об’ємами використання такого підходу повинно бути досліджене.

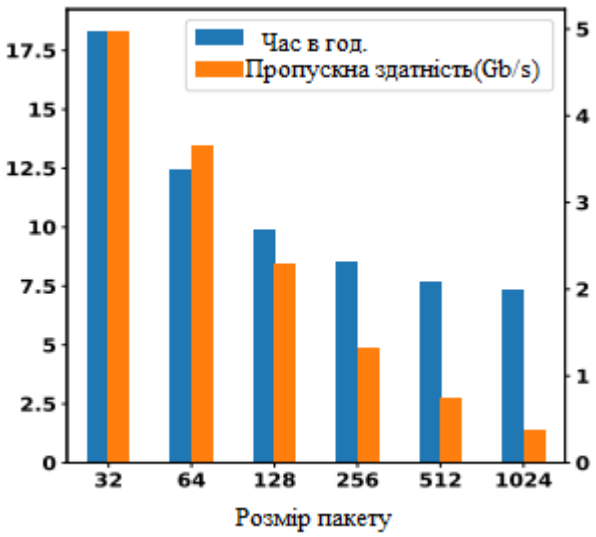


Рис.4. Мінімальна пропускна здатність залежно від розміру пакету.

Висновок

Описані дослідження показують суттєвий приріст у продуктивності роботи із навчальними даними в лабораторних умовах, що теоретично із невеликою похибкою, може, бути отриманий і від реальної системи розпізнавання. Однак є певні необхідні умови, які роблять можливим отримання прискорення. Перенесення такого способу роботи на обчислювальні елементи менш продуктивні, але об'єднані між собою можуть показувати приріст за умови розподілення задачі відповідно до потужності кожного з елементів. Такий підхід може вимагати окремого балансувального модуля та має бути вивчений так само, як і доцільність такого варіанту роботи адже центральний балансувальний компонент системи є елементом притаманним для централізованої топології, хоча й не впливає безпосередньо на спосіб спілкування, отримання та передачі учнями, а більш коректне розподілення завдань, потенційно, може, дати додатковий приріст у швидкодії системи.

References

1. G Hinton, L Deng, D Yu, G Dahl, A Mohamed, N Jaitly, A Senior, V Vanhoucke, P Nguyen, T. N Sainath, and B Kingsbury, «Deep neural networks for acoustic modeling in speech recognition,» IEEE Signal Processing Maganize, pp. 82–97, November 2012.
2. G Saon, G Kurata, T Sercu, K Audhkhasi, S Thomas, D Dimitriadis, X Cui, B Ramabhadran, M Picheny, L.-L Lim, B Roomi, and P Hall, «English conversational telephone speech recognition by humans and machines,» in Interspeech, 2017.
3. W Xiong, J Droppo, X Huang, F Seide, M. L Seltzer, A Stolcke, D Yu, and G Zweig, «Toward human parity in conversational speech recognition,» IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 25, no. 12, pp. 2410–2423, Dec 2017.
4. P Goyal, P Dollar, R. B Girshick, P Noordhuis, L Wesolowski, ´ A Kyrola, A Tulloch, Y Jia, and K He, «Accurate, large minibatch SGD: training imagenet in 1 hour,» CoRR, vol. abs/1706.02677, 2017.
5. M Cho, U Finkler, S Kumar, D. S Kung, V Saxena, and D Sreedhar, «Powerai DDL,» CoRR, vol. abs/1708.02188, 2017.
6. Y You, I Gitman, and B Ginsburg, «Scaling SGD batch size to 32k for imagenet training,» CoRR, vol. abs/1708.03888, 2017.
7. X Jia, S Song, W He, Y Wang, H Rong, F Zhou, L Xie, Z Guo, Y Yang, L Yu, T Chen, G Hu, S Shi, and X Chu, «Highly scalable deep learning training system with mixed-precision: Training imagenet in four minutes,» CoRR, vol. abs/1807.11205, 2018.
8. W Wen, C Xu, F Yan, C Wu, Y Wang, Y Chen, and H Li, «Terngrad: Ternary gradients to reduce communication in distributed deep learning,» in NIPS'2017, pp. 1509–1519. Curran Associates, Inc., 2017.
9. F Seide, H Fu, J Droppo, G Li, and D Yu, «1-bit stochastic gradient descent and application to data-parallel distributed training of speech dnns,» in Interspeech 2014, September 2014.
10. D Amodei(et.al.), «Deep speech 2: End-to-end speech recognition in english and mandarin,» in ICML'16. 2016, pp. 173–182, PMLR.

11. X Lian, W Zhang, C Zhang, and J Liu, «Asynchronous decentralized parallel stochastic gradient descent,» in ICML, 2018.
12. W Zhang, S Gupta, X Lian, and J Liu, «Staleness-aware async-sgd for distributed deep learning,» in Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence, IJCAI 2016, New York, NY, USA, 9–15 July 2016, 2016, pp. 2350–2356.
13. P Patarasuk and X Yuan, «Bandwidth optimal all-reduce algorithms for clusters of workstations,» J. Parallel Distrib. Comput., vol. 69, pp. 117–124, 2009.
14. Baidu, Effectively Scaling Deep Learning Frameworks, Available at https://github.com/baidu-research/ baidu-allreduce.
15. Nvidia, NCCL: Optimized primitives for collective multiGPU communication, Available at https://github.com/ NVIDIA/nccl.

ПРАВИЛА ОФОРМЛЕННЯ СТАТЕЙ

Статті подаються в обсязі 7-12 сторінок формату А4, не більше 4 -х авторів.

Текст в редакторі Word, шрифт –Arial , 11 пт, інтервал - 1, розміри полів: ліве - 2,5 см., праве - 1 см. Абзаци- 0,75 см. Формули у внутрішньому редакторі MS Office Word.

Порядок оформлення: УДК 11 пт, назва статті заголовним 12 пт, ПІБ-все жирно ; назва університету, місто, країна, e-mail ,10 п. –все курсивом.

Анотації курсивом 10 п. Слово «Анотація» жирно.

В статті мають бути розділи: вступ, дослідження або розробка, висновки. Заголовки 11 п. жирно.

Підпис рисунків і таблиць 10 п.

В кінці наводиться список літератури, 9 п, не більше 15 джерел. . Оформлення літератури за стандартом ДСТУ 8302:2015.

ARTICLE DESIGN RULES

Articles are submitted in the amount of 7-12 pages of A4 format, no more than 4 authors.

Text in Word editor, font - Arial, 11 pt, spacing - 1, field sizes: left - 2.5 cm, right - 1 cm. Paragraphs - 0.75 cm. Formulas in the internal editor MS Office Word.

Procedure: UDC 11 pt, title of the article heading 12 pt, full name, everything is bold; name of university, city, country, e-mail, 10 points - all in italics.

Annotations in italics 10 n. The word "Abstract" is bold.

The article should have sections: introduction, research or development, conclusions. Headings 11 sts bold.

Caption of figures and tables 10 p.

At the end is a list of references, 9 items, no more than 15 sources. . Registration of literature according to the standard DSTU 8302: 2015.

Тираж 50 пр. Зам. № …..

Сайт: visn-icct.uu.edu.ua/

E-mail: infcct@ukr.net

Адреса редакції: *м. Київ, вул. Львівська, 23, тел. (044) 424-62-74*

Відповідальний редактор *Семенко А.І.*

Комп’ютерна верстка *Войтенко В.М*

Дизайн обкладинки *Бабинець Н.А.*

Видавець і виготовлювач університет «Україна»

03115, м. Київ, вул. Львівська, 23, тел./факс (044) 424-24-14, 424-56-26

E-mail: ukraina.vdk@email.ua

Свідоцтво суб’єкта видавничої справи ДК №405 від 06.04.01