e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2020. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2020. № 1

UDC 004.058.5

METHOD OF DATA DEPERSONALIZATION IN PROTECTED AUTOMATED INFORMATION SYSTEMS

Spevakov A. G. – PhD, Associate Professor of the Information Security Department, Southwest State University, Kursk, Russian Federation.

Spevakova S. V. – Post-graduate student of the Computer Science Department, Southwest State University, Kursk, Russian Federation.

Primenko D. V. – Post-graduate student of the Computer Science Department, Southwest State University, Kursk, Russia.

ABSTRACT

Context. The problem of data depersonalization in information systems is considered. The analysis of modern approaches to depersonalization of data is carried out, it is revealed and proved by need of creation of the new method allowing to increase security of the processed data and their reliability. The object of the study was a model of data depersonalization, allowing to reduce the cost of protecting information systems.

Objective. The goal of the work is the analysis of modern methods of depersonalization and the creation of a method that eliminates the identified shortcomings, with an increased level of confidentiality and use of hashing of critical data and a private key.

Method. A method of personal data depersonalization is proposed, based on the method of entering identifiers using hashing of critical data and a private key, which allows to increase the confidentiality of information processed in information systems. Methods are proposed for selecting key critical attributes from primary documents that uniquely identify the subject of personal data, the method of generating initial sets, which divides the source data into two disjoint subsets, the method of generating a hash identifier from a unique sequence and a private key that depersonalizes information and enhances its confidentiality.

Results. The developed method is implemented in software and researched while solving the problems of depersonalization.

Conclusions. The carried out experiments confirmed the efficiency of the proposed method and allow to recommend it for implementation in automated information systems for processing personal data for solving problems of depersonalization. Prospects for further research may be in the creation of hardware streamlined data depersonalization allowing to increase the speed of processing and confidentiality of data in the information systems.

KEYWORDS: depersonalization, personal data, hash identifier, hash algorithm, private key, information system.

ABBREVIATIONS

PD is a personal data;

ISPD is an information system of personal data.

NOMENCLATURE

D is a personal data table;

M is a total amount of attributes;

N is a table rows count;

A_1 , A_2 are datasets;

K is a number of key attributes;

F is a hash function;

a_{ik} is a rows of data of the table;

P is an original message;

f is a multi-round non-key reshuffle;

$Theta, Chi, Pi, Rho, Lota$ are hash functions;

A, B, C, D are arrays;

x is an amount;

i is a counter;

Z is a hashing results;

r is an array defining the count of bits of reshuffle for each state;

PK is a private key.

INTRODUCTION

In modern automated systems a large amount of personal data of various security classes is processed. In accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, January 28, 1981) (with changes and additions), the operator must ensure the confidentiality of the data being processed, which leads to significant material costs [1–3]. So the cost of protecting one workplace of an automated personal data processing system can be more than 1000 US dollars, and the number of workstations of an automated system can be several hundreds of dollars. Also the problem faced by many companies, collecting and storing consents to the processing of personal data that require handwritten completion or using an electronic signature, is known. To solve this problem, the methods of depersonalization can be used [4].

The object of the research is the process of transforming confidential personal data into anonymous, non-confidential sequence.

The process of converting confidential personal data into an impersonal non-confidential sequence usually takes a lot of time, has a low resistance to attacks and has limitations at processing large amounts of personal data with frequent changes.

The subject of the research is the methods of deflating personal data.

Known methods of data depersonalization [5–8] have low speed; in records relationships between attributes of depersonalized data and their corresponding personal data attributes are partially preserved; if the values of individual attributes change, only the composition of the data can change, not the depersonalization. Therefore, in order to increase the speed and confidentiality of data depersonalization, it is necessary to develop a method to eliminate the identified shortcomings.

DOI 10.15588/1607-3274-2020-1-16

The purpose of the work is to increase the speed and quality of the process of depersonalization of data processed in automated information systems.

1 PROBLEM STATEMENT

Let us assume that the raw data is given in a form of preliminary values $D_N(d_1, d_2, ..., d_M)$, where M is the total attribute count and N is the table row count. Attributes d may be key and non-key. As the result the number of the key values is equal to $K\ (0 < K < M)$. While forming of data for hashing a private key PK with bitness of 512 is used. For a given sequence of data, the depersonalization function can be represented as the task of splitting data into two sets, A_1 and A_2, wherein A_1 contains confidential data, A_2 the anonymous information, and finding a unique d_0 sequence such that, for set $F(a_{i1}, a_{i2}, \ldots, a_{ik}, PK)$, the value d_0 will be a unique $d_0 = const$. At the same time the following condition is met – the inverse is impossible, finding a $(a_{i1}, a_{i2}, \ldots, a_{ik}, PK)$ data block from any d_0 is impossible, which in turn allows to establish the interrelation of the elements of the first and second sets.

2 REVIEW OF THE LITERATURE

In the process of analysis of modern methods of PD depersonalization the following methods were studied: method of identifiers implementation, method of change of composition or semantic, method of decomposition, mixing method.

1) Method of identifiers implementation is a replacement of personal data values with creation of a table (guide) of conformity of identifiers with the initial data. The disadvantages of this method are:

a) In the request and in the response to this request the type of representation of PD attributes that were replaced with identifiers is changed.

b) In the records the relations between attributes of depersonalized data and PD attributes corresponding to them are saved.

c) It is applicable to a small amount of PD attributes and the small volume of a PD array.

2) Method of change of composition or semantics is the change of composition or semantics of personal data by replacement with statistic processing, transformation, compilation or replacement of some information [9]. This method has the next disadvantages:

a) Application of this method is uneffective for PD depersonalization, because during PD attributes extracting it is necessary to consider the possibility of depersonalization with the usage of these attributes.

b) During basic replacement of values of separate attributes only change of PD composition can happen, but not depersonalization.

c) In record relations between attributes of depersonalized data and the attributes of personal data corresponding to them are partially saved.

d) Applicable when processing tasks do not require personalization of depersonalized data, if it is needed this process can be used on small data arrays.

3) Method of decomposition is division of an array of personal data into several sub-arrays with subsequent separate storage of sub-arrays . The basic disadvantages are:

a) It saves relations between attributes of depersonalized data and PD attributes corresponding to them in records of each storage.

b) Is applicable on large arrays of PD.

c) Resistance to attacks depends on the complexity of setup of relations between tables

4) Mixing method is a reshuffle of separate values or groups of values of personal data attributed in an array of persona data. This method has these disadvantages:

a) This method does not save relations between attributes of depersonalized data and personal data attributes corresponding to them in records.

b) Resistance to attacks increases with growth of the size of the array of personal data.

c) In applicable to large arrays of personal data with frequent changes in data.

The algorithms for the implementation of the identifiers' priming method are represented by functions, some of which consider various cryptographic approaches for generating an identifier for the connection between the cross-reference table and the depersonalized database. For example, a unique and relevant identifier of an individual is obtained by using a one-way cryptographic function from the following attributes: the surname, name, patronymic and date of birth of the individual – O.A. Vishnyakova and D. N. Lavrov [9]. There is also a patent for a method of identifying a subject of personal data using a SIM card as an identifier for communication, proposed by E. S. Volokitina [10]. The method has been successfully implemented in educational organizations. The featured algorithm successfully solves the security problem during processing anonymous data. However, the use of an additional identifier complicates the processing and increases costs.

Algorithms for the implementation of a method of changing the composition or semantics are presented by I. Y. Kuchin [11], which proposes an approach of encoding identifying attributes based on the developed algorithm. A distinctive feature of the work is the analytical justification for the choice of the composition of the identifying group and the provision of a given degree of anonymity as part of an anonymous database. This method has been introduced in the healthcare field, however, the issue of ensuring security is solved only when storing personal data, not when dealing with other information processing modes.

Algorithms for the implementation of the mixing method are presented by works that propose the use of mixing algorithms aimed at the storage of PI or its transmission over open communication channels. For example, K. O. Bondarenko and V. A. Kozlov [12] have presented a method of mixing data inside segments with sequential

DOI 10.15588/1607-3274-2020-1-16

mixing of rows and sensitive attributes, as the algorithm uses lookup tables generated by the cryptographic gamma method. On the one hand, the use of cryptography guarantees the sustaining power of the algorithm even during a processing session, but, on the other hand, it complicates the process of adding, deleting, searching data and increases the cost of protection. These shortcomings are obstacles for the implementation of the method.

Other research areas involve the use of mainly cryptographic methods, which can be attributed to depersonalization with a sufficient degree of conditionality, since they solve the problem of the impossibility of identifying an individual according to the processed data, but they are not formally included in the set of methods established by Roskomnadzor or merely partially use such methods. For example, the work of Y. V. Trifonova and R. F. Zharinov [13] suggests using the built-in cryptographic tools of the CryptDB database management system. As an example of the partial use of the identifier method, one can cite the work of I. Azhmukhamedov, R. Y. Demina and I. V. Safarov [14], wherein the cross-reference table encryption is applied with subsequent blocking.

To generate a sequence hash, the following method is used based on the concept of a cryptographic sponge, which calls for two primary stages [15–16].

1) Absorbing. The initial message P is subject to multi-round reshuffles *f*, accumulation and processing of all blocks of the message from which the hash will be developed is conducted [17].

2) Squeezing. The output of the received value of Z as the shuffle result, the development of the hash value and the output of the results until the necessary length of the hash is reache [18].

In the absorbing phase first is set the initial state from the zero vector with the size up to 1600 bits . Next is conducted the operation xor of a fragment of the initial message p_0 with the fragment of the initial state with the size of r, the remaining part of the state with capacity of c remains the same.

The result is processed by the f function which is a multiround non-key pseudo-random reshuffle and repeats till the initial message blocks exhaust [19]. Next comes the squeezing phase at which it is possible to extract a hash of a random length. The flow chart of the hashing algorithm is shown at the Fig. 1.

The function $F()$ in this algorithm executes 24 rounds, one round includes the work of five functions *Theta,Chi,Pi,Rho,Lota*, consistently processing the inner state at each round.

The function *Theta* is represented by the next expressions (1):

$$C[x]=A[x,0]\oplus A[x,1]\oplus A[x,2]\oplus A[x,3]\oplus A[x,4], x=0\ ..4$$
$$D[x]=C[x-1]\oplus (C[x+1]>>>1), x=0\ ..4;$$
$$A[x,y]=A[x,y]\oplus D[x], x=0...4, y=0...4. \quad (1)$$

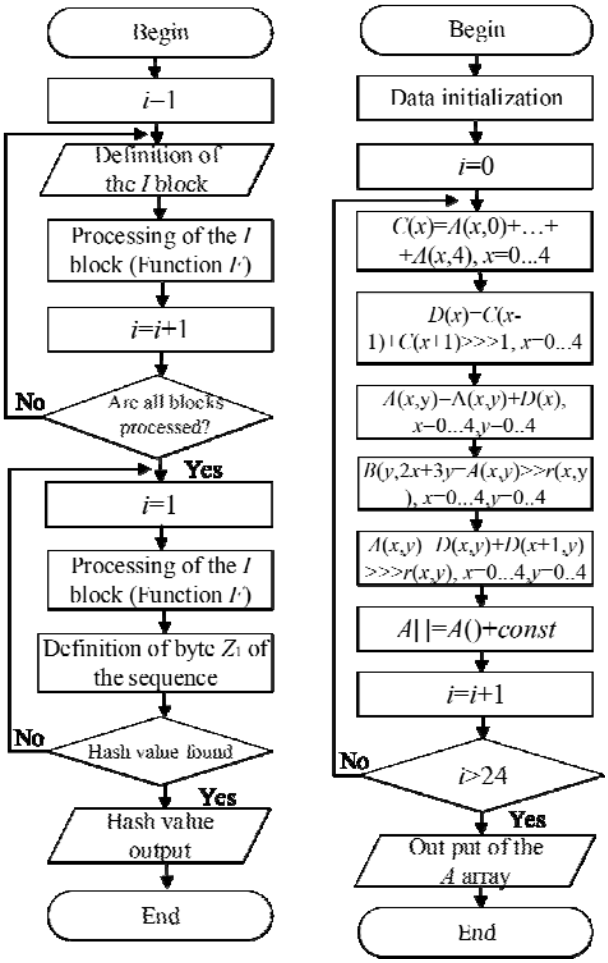


Figure 1 – The flow chart of the hashing algorithm

The function *Chi* is represented by the next expression (2):

$$A[x,y]=B[x,y]\oplus(\sim B[x+1,y]\&B[x+2,y], x=0..4, y=0..4. \quad (2)$$

The functions *Pi*, *Rho* are represented by the next expression (3):

$$B[y,2x+3y]=A[x,y]>>>r(x,y), x=0...4, y=0...4. \quad (3)$$

The function *Lota* is represented by the next expression (4):

$$A[0,0]=A[0,0]\ \text{xor}\ RC. \quad (4)$$

Where B is a temporary array having the same structure as the state array; C and D are the temporary arrays each containing 5 64-bit words; r -array defining the number of bits of spinage for each word of the state; inversion of the value $\sim B[x+1,y]$.

Step1: at the beginning of the algorithm data initialization is conducted. The size of the state is 1600 bits. Next to the variable i the value 0 is assigned.

Step2: after this the processing of the array with functions $C[x]$, $D[x]$, $A[x,y]$, $B[y,2x+3y]$, $A[x,y]$ begins, and besides these operations is conducted the summation of the xor-round constant RC with the word $A[0,0]$.

DOI 10.15588/1607-3274-2020-1-16

Step 3: after data processed with subfunctions goes the check for the rounds count. If the condition $i > 24$ is true then the output of the A array is conducted. If not then we increment by 1 and make the operations until this condition is true.

3 MATERIALS AND METHODS

In order to eliminate the drawbacks mentioned above a personal data depersonalization method, based on the method of identifiers implementation using hashing of critical data and a private key, was developed [20]. As raw data a personal data table $D_N(d_1, d_2, ..., d_M)$ is reviewed, where M is the total amount of attributes and N is table rows count, d_M is an attribute referring to key and non-key.

In this, at the first step by expert way critical data and data clearly identifying the personal data subject is defined. Corresponding attributes are defined as ley ones.

At the second step the initial array D according to chosen key attributes is split into two non-intersecting sub-arrays A_1 and A_2. It is worth noting that into each of sub-arrays an additional attribute d_0 is added, by which value later the comparison of depersonalized data with the personal data subject is conducted. As the result the number of key values is equal to K patients $(0 < K < M)$. . In this, in A_2 is stored depersonalized data that is not interesting for the intruder, so it does not require protection and is stored in the clear.

At the third step for the set of key values of each row $(a_{i1}, a_{i2}, \ldots, a_{in}) \in A_1$, where $i = 1,2,\ldots,N$ the value of the attribute $d_0 = F(a_{i1}, a_{i2}, \ldots, a_{ik}, PK)$ is calculated, where F is a unique function unknown for the user, PK is the unique private key. As F in this case the hash function is chosen [21].

$A_1(d_0, a_1, a_2, \ldots, a_n)$, $A_2(d_0, b_1, b_2, \ldots, b_n)$ where A_1 is the $(a_1, a_2, \ldots, a_n)$ set of confidential data and the d_0 hash, A_2 is the $(b_1, b_2, \ldots, b_n)$ set of anonymous data and the d_0 hash. In addition to the above, knowing the initial $(a_{i1}, a_{i2}, \ldots, a_{in}) \in A_1$ data can contribute to finding the $(b_{i1}, b_{i2}, \ldots, b_{in}) \in A_2$ set.

4 EXPERIMENTS

For the experiments a computer program and a database, implementing the proposed method, with the initial data of 100 subjects of personal data of a medical institution, were developed. The developed software has been studied at solving the problems of depersonalization.

On the basis of the initial sample, key critical attributes were identified that uniquely identify the subject of personal data that is stored in a protected information system. Using this data and a private key, for each record a hash identifier is generated, which is the primary key of the subject of the personal data in the depersonalized information system.

To search for the necessary record in an impersonal information system, a developed subprogram for calculating the identifier hash is used, which based on the data from the primary documents of the personal data subject formed the primary key of the specific record.

After the formation of data for a depersonalized information system, an analysis was performed for the presence of collisions [22–23].

5 RESULTS

As an example let's review a database of patients of some treatment institution (see table 1).

Table 1– Patient database

Last name	First Name	Patronymic	Sex	Date of birth	Medical insurance	Diagnosis
Ivanov	Ivan	Ivanovich	M	12.12.1992	12345678910	Pneumonia
Petrov	Denis	Yurievich	M	11.11.1990	46548677684	Pyelonephritis

For example, for the patient Ivanov the critical personal data is: first name, last name, patronymic, date of birth. For the hash identifier preparation we will use this data:
{Ivanov,Ivan,Ivanovich,12.12.1995}+{bPeShVkYp3s6v9y$B&E)H@McQfTjWnZq}, where the second addend is the private key of the treatment institution. After the calculation we get the hash identifier: 1628b3db5c13865aea5856a630a736653059fc7e2d7c49f897b636428c62a26b.

In the depersonalized database the hash identifier and the depersonalized personal data are stored (see table 2).

Table 2 – Depersonalized database

Hash identifier	Medical insurance	Diagnosis
1628b3db5c13865aea5856a630a736653059fc7e2d7c49f897b636428c62a26b	12345678910	Pneumonia
4d949d630cfaafe3dd151a2e06d7345a44a61889a8c097622abfd6ca0f515a7f	46548677684	Pyelonephritis

In the secure database the hash identifier and the critical personal data are stored (see table 3).

Table 3 – Secure database

Hash identifier	Last name	First name	Patronymic	Date of birth	Hash identifier
1628b3db5c13865aea5856a630a736653059fc7e2d7c49f897b636428c62a26b	Ivanov	Ivan	Ivanovich	12.12.1992	1628b3db5c13865aea5856a630a736653059fc7e2d7c49f897b636428c62a26b
4d949d630cfaafe3dd151a2e06d7345a44a61889a8c097622abfd6ca0f515a7f	Petrov	Denis	Yurievich	11.11.1990	4d949d630cfaafe3dd151a2e06d7345a44a61889a8c097622abfd6ca0f515a7f

DOI 10.15588/1607-3274-2020-1-16

In this, the ability to restore the original data from the hash identifier is impossible. To obtain an identifier it is required to fill in the necessary fields of the subject of personal data from primary documents using the private key in the developed software.

6 DISCUSSION

Let's consider the application of this method sing the famous characters Alice and Bob [24].

Alice came to see Doctor Bob. To identify Alice she shows Bob the critical PD from her initial documents (passport and medical insurance). Bob using the calculator for hash identifier inserts this data and the key of the hospital and forms the hash identifier that allows getting the access to Alice's patient file. After diagnosing and prescribing treatment Bob inserts data into the information system and sings it with his electronic signature.

A curious staff member Eva wanted to know Alice's diagnosis but can't find her card in the information system because she does not know the hash identifier as well as Alice's critical data.

Mallorie found out Alice's critical PD and got the access to the calculator for hash identifier, but she does not know the hospital's key for calculating Alice's identifier.

This method has the next advantages:

1) Data becomes depersonalized which reduces costs of ISPD protection.

2) It is impossible to define the presence of a certain subject in ISPD by known unique attributes.

3) Operator during subject's application by his PD gets access only to one record of ISPD.

4) The context analysis is impossible.

CONCLUSIONS

The actual problem of data depersonalization in the information system was solved by introducing identifiers using hashing of critical data and a private key.

The scientific novelty of the obtained results is that a method was proposed for introducing identifiers using hashing of critical data and a private key for the first time. This allows to increase the level of data confidentiality, reduce the requirements for the level of information system security, increase the speed of data processing by convolving critical data into a hash identifier.

The practical significance of the obtained results is that software that implements the proposed method has been developed and experiments have been carried out to confirm the adequacy of the proposed mathematical model. The results of the experiment allow us to recommend the proposed method for introducing into automated information systems the processing of personal data at the design stage or optimizing of the existing systems, which will reduce the cost of protecting the information system.

Prospects for further research are to explore the possibility of implementing this method in a software and hardware system that allows to increase the speed of the information system.

REFERENCES

1. Rodichev Yu. A. Normativnaya baza i standarty v oblasti informacionnoj bezopasnosti. Sankt-Peterburg, Izdatel'skij dom «Piter», 2018, 255 p.
2. Sychev Yu. V. Standarty informacionnoj bez-opasnosti. Zashchita i obrabotka konfidencial'nyh dokumentov. Saratov, Vuzovskoe obrazovanie, 2019, 223 p.
3. The Convention for the protection of individuals with regard to automatic processing of personal data is a 1981 Council of Europe [Electronic resource]. Access mode: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
4. Regulation (EU) 2016/679 of the European parliament and of the council GDPR(General Data Protection Regulations) [Electronic resource]. Access mode: https://ogdpr.eu/en/gdpr-2016-679.
5. Prikaz Roskomnadzora ot 05.09.2013 № 996 «Ob utverzhdenii trebovanij i metodov po obezlichi-vaniyu personal'nyh dannyh». [Elektronnyj resurs]. Rezhim dostupa: http://www.consultant.ru/document/cons_doc_LAW_151882/
6. Kalutskiy I. V., Shumailova V. A. , Nikulin D. A. et all. Depersonalization of personal data during processing of information in automated systems, *Telecommunications,* 2016, No. 10, pp. 16–20.
7. Spevakova S. V., Primenko D. V. A method of personal data depersonalization in automated systems, *Conference: Optoelectronic devices in pattern recognition systems, image processing and symbol information. Recognition – 2017, Kursk, 16–17 May 2017, proceeding*. Kursk, UZGY, 2017, pp. 330–333.
8. Dobritsa V. P., Gubarev A. A. Algorithm of exclusive transformation of data, *News of the Kursk State Technical University,* 2010, No. 1 (30), pp. 49–54.
9. Vishnyakova O. A., Lavrov D. N. Format obmena dannymi v sisteme sbora i obrabotki biometricheskih obrazcov, *Informacionnye resursy v obrazovanii: mater. mezhdunar. nauch.-prakt. konf*. Nizhnevartovsk, Izdatel'stvo Nizhnevart. gos. un-ta, 2013, pp. 146–149.
10. Volokitina E. S. Metod i algoritmy garantiro-vannogo obezlichivaniya i reidentifikacii sub'ekta personal'nyh dannyh v avtomatizirovannyh informacionnyh sistemah: dis. kand. tekhn. nauk. Sankt-Peterburg, Izdatel'stvo Sankt-Peterburgskogo nac. issled. un-ta informacionnyh tekhnologij, mekhaniki i optiki, 2013, 183 p.
11. Kuchin I. Yu. Obrabotka baz dannyh s personifi-cirovannoj informaciej dlya zadach obezlichivaniya i poiska zakonomernostej: dis. … kand. tekhn. nauk. Astrahan', Izdatel'stvo Astrah. gos. tekhn. un-ta, 2012, 132 p.
12. Bondarenko K. O., Kozlov V. A. Universal'nyj bystrodejstvuyushchij algoritm procedur obezlichivaniya dannyh, *Izv. YuFU. Tekhnicheskie nauki.* Rostov/n/D, Izdatel'stvo YuFU, 2015, No. 11 (172), pp. 130–142.
13. Trifonova Yu. V., Zharinov R. F. Vozmozhnosti obezlichivaniya personal'nyh dannyh v sistemah, ispol'zuyushchih relyacionnye bazy dannyh, *Doklady TUSUR*, 2014, No. 2 (32), pp. 188–194.
14. Azhmuhamedov I. M., Demina R. Yu., Safarov I. V. Sistemnyj podhod k obespecheniyu konfidencial'nosti obezlichennyh personal'nyh dannyh v uchrezhdeniyah zdravoohraneniya, *Sovremennye problemy nauki i obrazovaniya*, 2015, No. 1–1 [Elektronnyj recurs]. Rezhim dostupa: http://www.science-education.ru/ru/article/view?id=18610.
15. Bertoni G., Daemen J., Peeters M., Van G. Keccak code package [Electronic resource]. Access mode: https://github.com/gvanas/KeccakCodePackage
16. /[Huang S., Xu G., Wang M., et all Conditional cube attack on reduced-round Keccak sponge function Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, proceedings. Part II, 2017, P. 259–288.

DOI 10.15588/1607-3274-2020-1-16

17. Guo J., Liu M., Song L. Linear structures: Applications to cryptanalysis of round-reduced Keccak, *International Conference on the Theory and Application of Cryptology and Information Security*. Hanoi, Vietnam, December 4–8, 2016, proceedings. Part I, pp. 249– 274.
18. Jeethu J., Karthikab R., Nandakumarb R. Design and characterization of SHA 3–256 Bit IP core, *International conference on emerging trends in engineering, science and technology, ICETEST*, 2015, Vol. 24, pp. 918–924.
19. Dinur I., Morawiecki P., Pieprzyk J. et all. Cube attacks and cube-attack-like cryptanalysis on the round-reduced Keccak sponge function, *Eurocrypt: Annual International Conference on the Theory and Applications of Cryptographic Techniques Sofia*. Bulgaria, April 26–30, 2015, proceedings, Part I, pp. 733–761.
20. Nozdrina A. A., Spevakov A. G., Primenko D. V.; Patent RF 2636106, MPK G06F 12/14, G06F 12/14. Sposob depersonalizacii personal'nyh dannyh/ zayavitel' Yugo-Zapadnyj gosudarstvennyj universitet. № 2016126867; zayavl. 04.07.2016; opubl. 04.07.2016; Byul. № 32, 4 p.
21. Dobraunig C. Analysis of SHA-512/224 and SHA512/256 / C. Dobraunig, M. Eichlseder, F. Mende // International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 – December 3, 2015: proceedings. Part I, pp. 612–630.
22. Song L., Liao G., Guo J. Non-full sbox linearization: Applications to collision attacks on round-reduced Keccak, *Annual International Cryptology Conference.* Santa Barbara, CA, USA, August 20–24, 2017, proceedings. Part II, pp. 428–451.
23. Nabeel S., Munqath H. Anti-continuous collisions user based unpredictable iterative password salted hash encryption, *International Journal of Internet Technology and Secured Transactions,* 2018, Vol. 8, No. 4, pp. 619–634.
24. Barakat M., Eder Ch., Hanke T. An Introduction to Cryptography, [Electronic resource]. Access mode: https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

Received 11.06.2019.
Accepted 23.01.2020.

УДК 004.058.5

МЕТОД ЗНЕОСОБЛЕННЯ ДАНИХ В ЗАХИЩЕНИХ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Спеваков О. Г. – канд. техн. наук, доцент кафедри інформаційний безпеки, Південно-Західний державний університет, м. Курськ, Росія.
Спевакова С. В. – аспірант кафедри обчислювальної техніки, Південно-Західний державний університет, м. Курськ, Росія.
Применко Д. В. – аспірант кафедри обчислювальної техніки, Південно-Західний державний університет, м. Курськ, Росія.

АНОТАЦІЯ

Актуальність. Розглянуто завдання знеособлення даних в інформаційних системах. Проведено аналіз сучасних підходів до знеособлювання даних, виявлено та обґрунтовано необхідністю створення нового методу, що дозволяє підвищити захищеність оброблюваних даних і їх достовірність. Об'єктом дослідження є модель деперсоналізації даних, що дозволяє знизити витрати на захист інформаційних систем. Мета роботи – аналіз сучасних методів знеособлення і створення методу, що усуває виявлені недоліки, з підвищеним рівнем конфіденційності та використанням хешування критично важливих даних і приватного ключа.

Мета: аналіз сучасних методів знеособлення і створення методу, що усуває виявлені недоліки, з підвищеним рівнем конфіденційності та використанням хешування критично важливих даних і приватного ключа.

Метод. Запропоновано метод знеособлення персональних даних, заснований на методі введення ідентифікаторів з використанням хешування критично важливих даних і приватного ключа, що дозволяє досягти підвищення конфіденційності інформації, оброблюваної в інформаційних системах. Запропоновано методи вибору ключових критично важливих атрибутів з первинних документів, що дозволяють однозначно ідентифікувати суб'єкта персональних даних, методу формування вихідних множин, розбиває вихідні дані на два непересічних підмножини, методу формування хеш ідентифікатора з унікальної послідовності і приватного ключа, обезлічівающего інформацію і підвищує її конфіденційність.

Результати. Розроблений метод реалізований програмно і досліджений при вирішенні завдань знеособлення.

Висновки. Проведені експерименти підтвердили працездатність запропонованого методу та дозволяють рекомендувати його для впровадження в автоматизованих інформаційних системах обробки персональних даних для вирішення завдань знеособлення. Перспективи подальших досліджень можуть полягати у створенні апаратних засобів потокового знеособлення даних, що дозволяють підвищити швидкість обробки і конфіденційність даних в інформаційних системах.

КЛЮЧОВІ СЛОВА: знеособлення, персональні дані, хеш ідентифікатор, алгоритм хешування, приватний ключ, інформаційна система.

УДК 004.058.5

МЕТОД ОБЕЗЛИЧИВАНИЯ ДАННЫХ В ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Спеваков А. Г. – канд. техн. наук, доцент кафедры информационный безопасности, Юго-Западный государственный университет, г. Курск, Россия.
Спевакова С. В. – аспирант кафедры вычислительной техники, Юго-Западный государственный университет, г. Курск, Россия.
Применко Д. В. – аспирант кафедры вычислительной техники, Юго-Западный государственный университет, г. Курск, Россия.

АННОТАЦИЯ

Актуальность. Рассмотрена задача обезличивания данных в информационных системах. Проведен анализ современных подходов к обезличиванию данных, выявлена и обоснована необходимостью создания нового метода, позволяющего повысить защищенность обрабатываемых данных и их достоверность. Объектом исследования являлась модель деперсонализации данных, позволяющая снизить затраты на защиту информационных систем. Цель работы – анализ современных методов обезличивания и создания метода, устраняющего выявленные недостатки, с повышенным уровнем конфиденциальности и использованием хеширования критически важных данных и приватного ключа.

Цель работы: анализ современных методов обезличивания и создания метода, устраняющего выявленные недостатки, с повышенным уровнем конфиденциальности и использованием хеширования критически важных данных и приватного ключа.

Метод. Предложен метод обезличивания персональных данных, основанный на методе введения идентификаторов с использованием хеширования критически важных данных и приватного ключа, позволяющего добиться повышения конфиденциальности

DOI 10.15588/1607-3274-2020-1-16

информации, обрабатываемой в информационных системах. Предложены методы выбора ключевых критически важных атрибутов из первичных документов, позволяющих однозначно идентифицировать субъекта персональных данных, метода формирования исходных множеств, разбивающий исходные данные на два непересекающихся подмножества, метода формирования хэш идентификатора из уникальной последовательности и приватного ключа, обезличивающего информацию и повышающего её конфиденциальность.

Результаты. Разработанный метод реализован программно и исследован при решении задач обезличивания.

Выводы. Проведенные эксперименты подтвердили работоспособность предложенного метода и позволяют рекомендовать его для внедрения в автоматизированных информационных системах обработки персональных данных для решения задач обезличивания. Перспективы дальнейших исследований могут заключаться в создании аппаратных средств поточного обезличивания данных, позволяющих повысить скорость обработки и конфиденциальность данных в информационных системах.

КЛЮЧЕВЫЕ СЛОВА: обезличивание, персональные данные, хеш идентификатор, алгоритм хеширования, приватный ключ, информационная система.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности / Ю. А. Родичев. – Санкт-Петербург : Издательский дом «Питер», 2018. – 255 р.
2. Сычев Ю. В. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. В. Сычев. – Саратов : Вузовское образование, 2019. – 223 р.
3. The Convention for the protection of individuals with regard to automatic processing of personal data is a 1981 Council of Europe [Electronic resource]. – Access mode: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
4. Regulation (EU) 2016/679 of the European parliament and of the council GDPR(General Data Protection Regulations) [Electronic resource]. – Access mode: https://ogdpr.eu/en/gdpr-2016-679.
5. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_151882/.
6. Depersonalization of personal data during processing of information in automated systems/ [I. V. Kalutskiy, V. A. Shumailova, D. A. Nikulin et al.] // Telecommunications. –2016. – № 10. – P. 16–20.
7. Spevakova S. V. A method of personal data depersonalization in automated systems / S. V. Spevakova, D. V. Primenko // Conference: Optoelectronic devices in pattern recognition systems, image processing and symbol information. Recognition – 2017, Kursk, 16–17 may 2017 : proceeding: Kursk, UZGY, 2017. – P. 330–333.
8. Dobritsa V. P. Algorithm of exclusive transformation of data /V. P. Dobritsa, A. A. Gubarev// News of the Kursk State Technical University. – 2010. –№ 1 (30). – P. 49–54.
9. Вишнякова О.А. Формат обмена данными в системе сбора и обработки биометрических образцов / О. А. Вишнякова, Д. Н. Лавров // Информационные ресурсы в образовании: матер. междунар. науч.-практ. конф. – Нижневартовск : Издательство Нижневарт. гос. ун-та, 2013. – С. 146–149.
10. Волокитина Е. С. Метод и алгоритмы гарантированного обезличивания и реидентификации субъекта персональных данных в автоматизированных информационных системах: дис. канд. техн. наук / Е. С. Волокитина. – СПб. : Издательство Санкт-Петербургского нац. исслед. ун-та информационных технологий, механики и оптики, 2013. – 183 с.
11. Кучин И. Ю. Обработка баз данных с персонифицированной информацией для задач обезличивания и поиска закономерностей: дис. … канд. техн. наук / И. Ю. Кучин. – Астрахань : Издательство Астрах. гос. техн. ун-та, 2012. – 132 с.
12. Бондаренко К. О. Универсальный быстродействующий алгоритм процедур обезличивания данных / К. О. Бондаренко, В. А. Козлов // Изв. ЮФУ. Технические науки. – Ростов/н/Д: Издательство ЮФУ. – 2015. – № 11 (172). – С. 130–142.
13. Трифонова Ю. В. Возможности обезличивания персональных данных в системах, использующих реляционные базы данных / Ю. В. Трифонова, Р. Ф. Жаринов // Доклады ТУСУР. – 2014. – № 2 (32). – С. 188–194.
14. Ажмухамедов И. М. Системный подход к обеспечению конфиденциальности обезличенных персональных данных в учреждениях здравоохранения / И. М. Ажмухамедов, Р. Ю. Демина, И. В. Сафаров // Современные проблемы науки и образования. – 2015. – № 1–1 [Электронный ресурс]. – Режим доступа: http://www.science-education.ru/ru/article/view?id=18610.
15. Keccak code package [Electronic resource] / [G. Bertoni, J. Daemen, M. Peeters, G. Van]. – Access mode: https://github.com/gvanas/KeccakCodePackage
16. Conditional cube attack on reduced-round Keccak sponge function / [S. Huang, G. Xu, M. Wang et all.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 – May 4, 2017: proceedings. Part II, 2017. –P. 259–288.
17. Guo J. Linear structures: Applications to cryptanalysis of round-reduced Keccak / J. Guo, M. Liu, L. Song // International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4–8, 2016: proceedings. Part I. –P. 249– 274.
18. Jeethu J. Design and characterization of SHA 3– 256 Bit IP core / J. Jeethu, R. Karthikab, R. Nandakumarb // International conference on emerging trends in engineering, science and technology, ICETEST. – 2015. – Vol. 24. –P. 918–924.
19. Cube attacks and cube-attack-like cryptanalysis on the round-reduced Keccak sponge function / [I. Dinur, P. Morawiecki, J. Pieprzyk et al.] // Eurocrypt: Annual International Conference on the Theory and Applications of Cryptographic Techniques Sofia, Bulgaria, April 26–30, 2015: proceedings. Part I. – P. 733–761.
20. Патент РФ 2636106, МПК G06F 12/14, G06F 12/14. Способ деперсонализации персональных данных/ А. А. Ноздрина, А. Г. Спеваков, Д. В. Применко; заявитель Юго-Западный государственный университет. – № 2016126867; заявл. 04.07.2016; опубл. 04.07.2016; Бюл. № 32. – 4 с.
21. Dobraunig C. Analysis of SHA-512/224 and SHA512/256 / C. Dobraunig, M. Eichlseder, F. Mende // International Conference on the Theory and Application of Cryptology and Information Security, Auckland. – New Zealand, November 29 – December 3, 2015: proceedings. Part I. –P. 612–630.
22. Song L. Non-full sbox linearization: Applications to collision attacks on round-reduced Keccak / L. Song, G. Liao, J. Guo // Annual International Cryptology Conference. – Santa Barbara, CA, USA, August 20–24, 2017: proceedings. Part II. – P. 428–451.
23. Nabeel S. Anti-continuous collisions user based unpredictable iterative password salted hash encryption / S. Nabeel, H. Munqath // International Journal of Internet Technology and Secured Transactions. – 2018. – Vol. 8, № 4. –P. 619–634.
24. Barakat M. An Introduction to Cryptography, [Electronic resource] / M. Barakat, Ch. Eder, T. Hanke. – Access mode: https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

DOI 10.15588/1607-3274-2020-1-16

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2020. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2020. № 1

UDC 004.6

MULTIMODAL DATA PROCESSING BASED ON ALGEBRAIC SYSTEM OF AGGREGATES RELATIONS

Yevgeniya Sulema – PhD, Associate Professor in the Computer Systems Software Department, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

ABSTRACT

Context. In many engineering tasks where the monitoring of changes in the characteristics of an observation object, subject, or process is required, it is necessary to process multimodal data recorded with respect to time moments when these characteristics are registered. In this paper, the author presents a new approach to solving the problem of multimodal data structures timewise processing, which allows to simplify the processing of such data by using the mathematical apparatus of an algebraic system of aggregates and thereby reduce the requirements to computing resources. The algebraic system of aggregates operates with such specific data structures as aggregates and multi-images. These complex data structures can be obtained as a result of data measuring, generating, recording, etc. The processing of such multimodal data can also require discrete intervals processing.

Objective. The goal of the work is to formalise the relations between basic mathematical objects defined in the algebraic system of aggregates, such as elements, tuples and aggregates, as well as the data structures based on these mathematical objects, namely, discreet intervals and multi-images.

Method. The research presented in this paper is based on both the algebraic system of aggregates and the concept of multi-image which enable multimodal data timewise processing. A carrier of the algebraic system of aggregates is an arbitrary set of specific structures – aggregates. An aggregate is a tuple of arbitrary tuples, elements of which belong to predefined sets. Aggregates can be processed by using logical, ordering, and arithmetical operations defined in the algebraic system of aggregates. A multi-image is a non-empty aggregate, the first tuple of which is a tuple of time values. Such tuple of time values represents a certain discrete interval. To process discrete intervals and multi-images, a set of relations is defined in the algebraic system of aggregates. This set includes relations between tuple elements, relations between tuples, and relations between aggregates. The relations between tuples enable arithmetical comparison, frequency comparison, and interval comparison. This mathematical apparatus can be used for both complex representation of object (process) multimodal characteristics and further timewise processing of data represented as multi-images.

Results. The approach to discrete intervals and multi-images processing based on relations, which are defined in the algebraic system of aggregates, has been developed and presented in the paper. The author provides examples of the developed approach practical implementation.

Conclusions. The results obtained in the research presented in this paper has shown that the relations defined in algebraic system of aggregates enable processing of complex data structures named multi-images in data modelling, prediction and other tasks. To allow data processing with respect to time scale, discrete intervals can be employed. A discrete interval is a tuple of time values. In the paper, the author shows how relations for discrete intervals comparison can be used for solving practical tasks. Besides, the author presents the software tools which can be used for practical implementation of the given theoretical approach by employing the domain-specific language ASAMPL.

KEYWORDS: Multimodal Data Processing, Aggregate, Multi-Image, Discrete Interval.

ABBREVIATIONS

ASA is the algebraic system of aggregates;

ASAMPL is the programming language for mulsemedia data processing based on algebraic system of aggregates.

NOMENCLATURE

A is an aggregate;

$\mathscr{M}$ is a non-empty set (carrier);

$\mathscr{F}$ is a set of operations;

$\mathscr{R}$ is a set of relations;

i, i_1, i_2, j, k, q, p are indices;

$\overline{a}$, $\overline{a^1}$, $\overline{a^2}$, $\overline{a^j}$, $\overline{a_t}$, $\overline{a_p}$ are tuples of arbitrary values;

$\overline{t^1}$, $\overline{t^2}$ are tuples of time values;

$\overline{d_t^1}$, $\overline{d_t^2}$ are tuples of temperature values;

$\overline{d_p^1}$, $\overline{d_p^2}$ are tuples of pulse values;

$\overline{d_{sp}^1}$ is a tuple of systolic pressure values;

$\overline{d_{dp}^1}$ is a tuple of diastolic pressure values;

a_i^j, a_i^k, a_i^1, a_i^2, $a_{i_1}^1$, $a_{i_2}^2$, a_p^1, a_q^1, a_p^2, a_q^2, a_e^1, a_e^2, $a_{n_1}^1$, $a_{n_2}^2$ are tuple elements;

n_1, n_2, n_j are tuple lengths;

M_N, M_S, M_W, M_K, M_j are sets;

N, N_p, N_q, N_e are powers of sets;

T is a set of time values;

τ is a time value;

I, I_1, I_2 are multi-images;

M_t is a set of temperature values;

M_p is a set of pulse values;

M_{sp} is a set of systolic pressure values;

M_{dp} is a set of diastolic pressure values.

INTRODUCTION

Nowadays, there is a wide range of tasks in engineering, health care, education, and other fields [1–3], where data are complex structures, values of which are defined,

DOI 10.15588/1607-3274-2020-1-17

measured, generated, recorded in terms of time. Since such data can be obtained in arbitrary time moments as well as they are a subject of digital processing in computer systems, time readings defining moments when certain data values are obtained are digital values which belong to discrete intervals.

Complex data in this context can be presented as a multi-image [4–6]. A multi-image is a complex representation of multiple data sets describing an object (subject, process) of observation which are obtained (measured, generated, recorded) in the course of time. In mathematical sense, the multi-image is an aggregate, the first data tuple of which is a non-empty tuple of time values. These values can be natural numbers or values of any other type which can be used for evident and monosemantic representation of time. The advantage of multi-image use is that since we have a complex representation of multimodal data sequences defined in terms of time, it gives new opportunities for data modelling, prediction and other similar tasks. To process multi-images, we need to operate with relations between them and their components. Since a multi-image is an aggregate, relations defined in the Algebraic System of Aggregates (ASA) are used. In this paper we present the relations of ASA and propose a general approach for their use.

The object of study is the process of multimodal data processing with respect to time stamps of data values.

The subject of study is relations between components of complex data structures, namely, between discrete intervals and between multi-images.

The purpose of the work is to formalise logical apparatus of the algebraic system of aggregates and elaborate an approach to its practical implementation.

1 PROBLEM STATEMENT

Let tuples $\overline{a^1} = \left\langle a_i^1 \right\rangle_{i=1}^{n_1}$ and $\overline{a^2} = \left\langle a_i^2 \right\rangle_{i=1}^{n_2}$, elements of which are unique discrete values such as either $a_i^k < a_{i+1}^k$, or $a_i^k > a_{i+1}^k$ is true for all pairs (a_i^k, a_{i+1}^k), $\forall i \in [1\,..\,n-1]$, $a_i^k \in \mathbb{R}$, $k = [1, 2]$ be discrete intervals. Then the problem is to establish relations between these discrete intervals which enable their arithmetical, frequency, and interval comparison which can be used for multi-image logical processing.

2 REVIEW OF THE LITERATURE

The foundations of interval algebra and interval-based temporal logic were presented in [7] where Allen proposed 13 relations between intervals. Allen and Hayes [8] extended Allen's interval-based theory by formally defining the beginnings and endings of intervals which have properties normally associated with points.

Nebel and Bürckert, in [9], introduced a new subclass of Allen's interval algebra called ORD-Horn subclass. The authors proved that reasoning in the ORD-Horn subclass is a polynomial-time problem and showed that the path-consistency method is sufficient for deciding satisfiability. Allen and Ferguson, in [10], presented a representation of events and actions based on interval temporal logic. One of important features of the logic is that it can express complex temporal relations because of its underlying temporal logic.

In [11], Schockaert, De Cock, and Kerre formulated a notion of a fuzzy time interval and proposed fuzzy Allen relations which are the generalization of Allen's interval relations. The authors applied the relatedness measures to define fuzzy temporal relations between vague events.

In [12], Bozzelli et al. studied the expressiveness of Halpern and Shoham's interval temporal logic which is "interval-wise" interpreted and enables expressing properties of computation stretches, spanning a sequence of states, or properties involving temporal aggregations, which are inherently "interval-based". Grüninger and Li, in [13], identified the first-order ontology that is logically synonymous with Allen's interval algebra, so that there is a one-to-one correspondence between models of the ontology and solutions to temporal constraints that are specified using the temporal relations.

These and other similar researches consider time as intervals and moments as well as such time values considered as single data, without structuring with data of other types. Thus, in our research we work on another approach which stipulates complex representation of multimodal data as aggregates and multi-images.

3 MATERIALS AND METHODS

ASA is an algebraic system, a carrier of which is an arbitrary set of specific structures – aggregates [4, 5].

Definition 1. An aggregate A is a tuple of arbitrary tuples, elements of which belong to predefined sets:

$$A = [\![M_j \mid \left\langle a_i^j \right\rangle_{i=1}^{n_j}]\!]_{j=1}^{N} = [\![\{A\} \mid \langle A \rangle]\!], \qquad (1)$$

where $\{A\}$ is a tuple of sets M_j, $\langle A \rangle$ is a tuple of elements tuples $\left\langle a_i^j \right\rangle_{i=1}^{n_j}$ corresponding to the tuple of sets ($a_i^j \in M_j$).

Since ASA is an algebraic system [14], it consists of sets $(\mathscr{M}, \mathscr{F}, \mathscr{R})$,, where $\mathscr{M}$ is a non-empty set (carrier), elements of which are elements of the system; $\mathscr{F}$ is a set of operations; $\mathscr{R}$ is a set of relations. The carrier of ASA is an arbitrary set of specific structures called aggregates.

Aggregates can be compatible, quasi-compatible or incompatible [4, 5].

Operations on aggregates include logical operations, ordering operations, and arithmetical operations.

The logical operations on aggregates are: Union, Intersection, Difference, Symmetric Difference, and Exclusive Intersection [4].

Ordering operations include: Sets Ordering, Sorting, Singling, Extraction, and Insertion [5].

DOI 10.15588/1607-3274-2020-1-17

Arithmetical operations include: Elementwise Addition, Scalar Addition, Elementwise Subtraction, Scalar Subtraction, Elementwise Multiplication, Scalar Multiplication, Elementwise Division, and Scalar Division.

The basic relations in ASA [4, 5] includes Is Equal, Is Less, Is Greater, Is Equivalent, Includes, Is Included, Precedes, Succeeds. Let us present the whole set of the relations in detail.

Relations in ASA include:
– Relations between tuple elements;
– Relations between tuples;
– Relations between aggregates.

Relations between tuple elements are Is Greater (>), Is Less (<), Is Equal (=), Proceeds ($\prec$), Succeeds ($\succ$). The first three relations (<, >, and =) are based on elements value and the last two relations ($\prec$ and $\succ$) concern elements position in a tuple. Naturally, elements must belong to the same tuple.

Let us consider elements of the following tuple:

$$\overline{a} = \langle a_1, a_2, a_3, a_4 \rangle = \langle 11,9,11,18 \rangle .$$

Then we can establish the fact of the following relations between the tuple elements:

$$a_1 > a_2 \; ; \; a_3 < a_4 \; ; \; a_1 = a_3 \; ; \; a_1 \prec a_2 \; ; \; a_3 \succ a_2 .$$

Relations between tuples enable the following types of tuples comparison:
- Arithmetical comparison;
- Frequency comparison;
- Interval comparison.

Arithmetical comparison can be applied to two tuples $\overline{a^1}$ and $\overline{a^2}$, where $\overline{a^1} = \left\langle a^1_{i_1} \right\rangle_{i_1=1}^{n_1}$ and $\overline{a^2} = \left\langle a^2_{i_2} \right\rangle_{i_2=1}^{n_2}$, if $a^1_{i_1} \in M$ and $a^2_{i_2} \in M$. Arithmetical comparison is elementwise and based on the following relations:
– Is Strictly Greater (>);
– Is Majority-Vote Greater ($\gg$);
– Is Strictly Less (<);
– Is Majority-Vote Less ($\ll$);
– Is Strictly Equal (=);
– Is Majority-Vote Equal (<>).

The relation Is Strictly Greater between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} > \overline{a^2} \text{ if } a^1_i > a^2_i, \; i = [1 \; .. \; n_1], \; n_1 = n_2. \qquad (2)$$

The relation Is Majority-Vote Greater between two tuples $\overline{a^1}$ and $\overline{a^2}$ can be defined as follows.

Let $N = \langle 1, 2, \ldots, n \rangle$, where

$$n = \begin{cases} n_1, \text{ if } n_1 \le n_2; \\ n_2, \text{ if } n_1 > n_2, \end{cases}$$

and let $\exists N_p \neq \varnothing$, $\exists N_q \neq \varnothing$ such as $N_p \cup N_q = N$, $N_p \cap N_q = \varnothing$ and $\left|N_p\right| > \left|N_q\right|$. Then $\forall p \in N_p$, $\forall q \in N_q$:

$$\overline{a^1} \gg \overline{a^2} \text{ if } a^1_p > a^2_p, \; a^1_q \le a^2_q . \qquad (3)$$

The relation Is Strictly Less between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} < \overline{a^2} \text{ if } a^1_i < a^2_i, \; \forall i = [1 \; .. \; n_1], \; n_1 = n_2 . \qquad (4)$$

The relation Is Majority-Vote Less between two tuples $\overline{a^1}$ and $\overline{a^2}$ can be defined as follows.

Let $N = \langle 1, 2, \ldots, n \rangle$, where

$$n = \begin{cases} n_1, \text{ if } n_1 \le n_2 \\ n_2, \text{ if } n_1 > n_2 \end{cases},$$

and let $\exists N_p \neq \varnothing$, $\exists N_q \neq \varnothing$ such as $N_p \cup N_q = N$, $N_p \cap N_q = \varnothing$ and $\left|N_p\right| < \left|N_q\right|$. Then $\forall p \in N_p$, $\forall q \in N_q$:

$$\overline{a^1} \ll \overline{a^2} \text{ if } a^1_p \ge a^2_p, \; a^1_q < a^2_q . \qquad (5)$$

The relation Is Strictly Equal between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} = \overline{a^2} \text{ if } a^1_i = a^2_i, \; \forall i = [1 \; .. \; n_1], \; n_1 = n_2 . \qquad (6)$$

The relation Is Majority-Vote Equal between two tuples $\overline{a^1}$ and $\overline{a^2}$ can be defined as follows.

Let $N = \langle 1, 2, \ldots, n \rangle$, where

$$n = \begin{cases} n_1, \text{ if } n_1 \le n_2; \\ n_2, \text{ if } n_1 > n_2, \end{cases}$$

and let $\exists N_e \neq \varnothing$, $\exists N_p \neq \varnothing$, $\exists N_q \neq \varnothing$ such as $N_p \bigcup N_q \bigcup N_e = N$, $N_p \bigcap N_q \bigcap N_e = \varnothing$ and $\left|N_e\right| > \left|N_p\right|$, $\left|N_p\right| = \left|N_q\right|$. Then $\forall p \in N_p$, $\forall q \in N_q$, $\exists e \in N_e$:

$$\overline{a^1} <> \overline{a^2} \text{ if } a^1_p > a^2_p, \; a^1_q < a^2_q, \; a^1_e = a^2_e . \qquad (7)$$

Let us consider the following tuples:

$$\overline{a^1} = \left\langle a^1_1, a^1_2, a^1_3, a^1_4 \right\rangle = \langle 11,9,11,18 \rangle ;$$
$$\overline{a^2} = \left\langle a^2_1, a^2_2, a^2_3, a^2_4 \right\rangle = \langle 2,7,4,10 \rangle ;$$

DOI 10.15588/1607-3274-2020-1-17

$$\overline{a^3} = \left\langle a_1^3, a_2^3, a_3^3, a_4^3, a_5^3 \right\rangle = \langle 7,19,4,10,8 \rangle;$$
$$\overline{a^4} = \left\langle a_1^4, a_2^4, a_3^4, a_4^4 \right\rangle = \langle 11,9,11,18 \rangle;$$
$$\overline{a^5} = \left\langle a_1^5, a_2^5, a_3^5, a_4^5, a_5^5 \right\rangle = \langle 14,9,11,10,8 \rangle.$$

Then we can establish the fact of the following arithmetical relations between these tuples:

$$\overline{a^1} > \overline{a^2};\ \overline{a^1} \gg \overline{a^3};\ \overline{a^2} < \overline{a^4};$$
$$\overline{a^3} \ll \overline{a^4};\ \overline{a^1} = \overline{a^4};\ \overline{a^1} <> \overline{a^5}.$$

Frequency comparison can be applied to two tuples $\forall\overline{a^1}$ and $\forall\overline{a^2}$ where $\overline{a^1} = \left\langle a_{i_1}^1 \right\rangle_{i_1=1}^{n_1}$ and $\overline{a^2} = \left\langle a_{i_2}^2 \right\rangle_{i_2=1}^{n_2}$. Frequency comparison is based on the following relations:

– Is Thicker ($\triangleright$);
– Is Rarer ($\triangleleft$);
– Is Equally Frequent ($\sim$).

The relation Is Thicker between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \triangleright \overline{a^2} \text{ if } \left|\overline{a^1}\right| > \left|\overline{a^2}\right|. \quad (8)$$

The relation Is Rarer between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \triangleleft \overline{a^2} \text{ if } \left|\overline{a^1}\right| < \left|\overline{a^2}\right|. \quad (9)$$

The relation Is Equally Frequent between two tuples $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \sim \overline{a^2} \text{ if } \left|\overline{a^1}\right| = \left|\overline{a^2}\right|. \quad (10)$$

Thus, if there are three tuples:

$$\overline{a^1} = \left\langle a_1^1, a_2^1, a_3^1, a_4^1, a_5^1 \right\rangle = \langle 14,9,15,18,6 \rangle;$$
$$\overline{a^2} = \left\langle a_1^2, a_2^2, a_3^2, a_4^2 \right\rangle = \langle 2,7,4,10 \rangle;$$
$$\overline{a^3} = \left\langle a_1^3, a_2^3, a_3^3, a_4^3, a_5^3 \right\rangle = \langle 7,19,4,10,8 \rangle.$$

Then $\overline{a^1} \triangleright \overline{a^2};\ \overline{a^2} \triangleleft \overline{a^3};\ \overline{a^1} \sim \overline{a^3}$.

To define how much thicker or how much rarer is a certain tuple in comparison with another tuple, we introduce a frequency measure which can be calculated as follows:

$$\eta = \frac{\left|\overline{a^1}\right|}{\left|\overline{a^2}\right|}. \quad (11)$$

For example, for tuples $\overline{a^1}$, $\overline{a^2}$ and $\overline{a^3}$ given above: $\eta_{12} = 1.25;\ \eta_{23} = 0.8;\ \eta_{13} = 1$.

Interval comparison can be applied to two tuples $\overline{a^1}$ and $\overline{a^2}$, where $\overline{a^1} = \left\langle a_{i_1}^1 \right\rangle_{i_1=1}^{n_1}$ and $\overline{a^2} = \left\langle a_{i_2}^2 \right\rangle_{i_2=1}^{n_2}$, if $a_{i_1}^1 \in M$ and $a_{i_2}^2 \in M$. Interval comparison [6] is based on relations of Allen's Interval Algebra. However, it has a significant difference from Allen's Interval Algebra in that it operates with discrete intervals. Let us define this notion and introduce the compact notation for relations between discrete intervals.

Definition 2. A discrete interval is a tuple, elements of which are unique values ordered either in ascending or in descending order.

The relation Is Before between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \leftarrow \overline{a^2} \text{ if } a_{n_1}^1 < a_1^2. \quad (12)$$

The relation Is After between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \rightarrow \overline{a^2} \text{ if } a_1^1 > a_{n_2}^2. \quad (13)$$

The relation Coincides With between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \leftrightarrow \overline{a^2} \text{ if } a_1^1 = a_1^2,\ a_{n_1}^1 = a_{n_2}^2 \text{ and } n_1 = n_2. \quad (14)$$

Note that this relation does not fully correspond to relation Equal of Allen's Interval Algebra because in ASA we deal with discrete intervals, thus, two discrete intervals can coincide in the first and last values, but other values can be unequal. For example, if we have two tuples $\langle 2,3,8,10 \rangle$ and $\langle 2,5,6,10 \rangle$, their discrete intervals coincide but are unequal.

The relation Meets between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \mapsto \overline{a^2} \text{ if } a_{n_1}^1 = a_1^2. \quad (15)$$

The relation Is Met By between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

DOI 10.15588/1607-3274-2020-1-17

$$\overline{a^1} \mapsto \overline{a^2} \text{ if } a^2_{n_2} = a^1_1 . \quad (16)$$

The relation Overlaps between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \leftrightarrow \overline{a^2} \text{ if } a^1_1 < a^2_1 \text{ and } a^1_{n_1} < a^2_{n_2} \text{ and } a^2_1 < a^1_{n_1} . \quad (17)$$

The relation Is Overlapped By between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \hookrightarrow \overline{a^2} \text{ if } a^2_1 < a^1_1 \text{ and } a^2_{n_2} < a^1_{n_1} \text{ and } a^1_1 < a^2_{n_2} . \quad (18)$$

The relation During between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \curvearrowleft \overline{a^2} \text{ if } a^1_1 > a^2_1 \text{ and } a^1_{n_1} < a^2_{n_2} . \quad (19)$$

The relation Contains between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \curvearrowright \overline{a^2} \text{ if } a^1_1 < a^2_1 \text{ and } a^1_{n_1} > a^2_{n_2} . \quad (20)$$

The relation Starts between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \leftarrowtail \overline{a^2} \text{ if } a^1_1 = a^2_1 \text{ and } a^1_{n_1} < a^2_{n_2} . \quad (21)$$

The relation Is Started By between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \rightarrowtail \overline{a^2} \text{ if } a^1_1 = a^2_1 \text{ and } a^1_{n_1} > a^2_{n_2} . \quad (22)$$

The relation Finishes between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \hookleftarrow \overline{a^2} \text{ if } a^1_1 > a^2_1 \text{ and } a^1_{n_1} = a^2_{n_2} . \quad (23)$$

The relation Is Finished By between two discrete intervals $\overline{a^1}$ and $\overline{a^2}$ is defined as follows:

$$\overline{a^1} \hookrightarrow \overline{a^2} \text{ if } a^1_1 < a^2_1 \text{ and } a^1_{n_1} = a^2_{n_2} . \quad (24)$$

Relations between aggregates consist of relations between sets of aggregates and relations between tuples of aggregates.

Relations between sets of aggregates are Is Equivalent ($\equiv$), Includes ($\supset$), Is Included ($\subset$).

The result of these relations depends of the aggregates compatibility [4, 5]. Let us consider aggregates A_1, A_2, A_3, A_4, A_5, and A_6 defined according to (1):

$$A_1 = [\![M_1, M_2, \ldots, M_N \mid \left\langle a^1_{i_1} \right\rangle_{i_1=1}^{n^1_1}, \ldots, \left\langle a^1_{i_N} \right\rangle_{i_N=1}^{n^1_N}]\!],$$

$$A_2 = [\![M_1, M_2, \ldots, M_N \mid \left\langle a^2_{i_1} \right\rangle_{i_1=1}^{n^2_1}, \ldots, \left\langle a^2_{i_N} \right\rangle_{i_N=1}^{n^2_N}]\!],$$

$$A_3 = [\![M_1, M^3_2, \ldots, M^3_S \mid \left\langle a^3_{i_1} \right\rangle_{i_1=1}^{n^3_1}, \ldots, \left\langle a^3_{i_S} \right\rangle_{i_S=1}^{n^3_S}]\!],$$

$$A_4 = [\![M^4_1, \ldots, M^4_W \mid \left\langle a^4_{i_1} \right\rangle_{i_1=1}^{n^4_1}, \ldots, \left\langle a^4_{i_W} \right\rangle_{i_W=1}^{n^4_W}]\!], \quad (25)$$

$$A_5 = [\![M_1, M_2 \mid \left\langle a^5_{i_1} \right\rangle_{i_1=1}^{n^5_1}, \left\langle a^5_{i_2} \right\rangle_{i_2=1}^{n^5_2}]\!],$$

$$A_6 = [\![M_2, M_1 \mid \left\langle a^6_{i_2} \right\rangle_{i_2=1}^{n^6_2}, \left\langle a^6_{i_1} \right\rangle_{i_1=1}^{n^6_1}]\!].$$

Thus, compatibility of the aggregates in (25) is as follows: $A_1 \doteqdot A_2$; $A_1 \doteq A_3$; $A_1 \doteq A_5$; $A_2 \doteq A_5$; $A_1 \triangleq A_4$; A_1 ($\doteqdot$) A_5.

Then relations between sets of these aggregates are: $\{A_1\} \equiv \{A_2\}$; $\{A_1\} \supset \{A_5\}$; $\{A_5\} \subset \{A_2\}$.

The rest of aggregates do not have these relations between their sets. It can be indicated by using negation:

$$\{A_1\} \not\equiv \{A_3\}; \{A_4\} \not\supset \{A_5\}; \{A_3\} \not\subset \{A_6\}.$$

Let us note that in spite of that {A1} $\not\supset$ {A3} the sets of these aggregates have common set M1. To establish

DOI 10.15588/1607-3274-2020-1-17

this fact formally, we can employ logical operation Intersection [4]: $\{A_1\} \cap \{A_3\} = M_1$ or more formally $\{A_1\} \cap \{A_3\} \neq \varnothing$.

Let us formulate relations between sets for any two aggregates.

The relation Is Equivalent between two aggregates A_1 and A_2 can be defined as:

$$\{A_1\} \equiv \{A_2\} \text{ if } A_1 \doteqdot A_2. \quad (26)$$

The relation Includes between two aggregates A_1 and A_2 can be defined as:

$$\{A_1\} \supset \{A_2\} \text{ if } A_1 \doteq A_2 \text{ and } |A_1| > |A_2|$$

$$\text{and } \{A_2\} = \langle M_1, \ldots, M_K \rangle, \langle M_1, \ldots, M_K \rangle \in \{A_1\}. \quad (27)$$

The relation Is Included between two aggregates A_1 and A_2 can be defined as:

$$\{A_1\} \subset \{A_2\} \text{ if } A_1 \doteq A_2 \text{ and } |A_1| < |A_2|$$

$$\text{and } \{A_1\} = \langle M_1, \ldots, M_K \rangle, \langle M_1, \ldots, M_K \rangle \in \{A_2\}. \quad (28)$$

Relations between tuples of aggregates are identical to relations between single tuples defined above relations of three types:

– Arithmetical relations;

– Frequency relations;

– Interval relations.

However, possibility of their application depends of the aggregates compatibility: relations between tuples can be established only for compatible and quasi-compatible aggregates.

Hiddenly compatible aggregates must be first transformed to compatible [5] and then a relation between tuples can be considered.

Let us also note that if tuples to be a subject of interval comparison are not discrete intervals (see Definition 2), at first, they must be sorted by using operator Sorting [5] and next they can be compared.

Relations between tuples of aggregates can be established with evident indication of the tuples to be compared:

$$\left\langle A_1(\overline{a^1}) \right\rangle \mapsto \left\langle A_2(\overline{a^1}) \right\rangle; \quad \left\langle A_1(\overline{a^2}) \right\rangle \ll \left\langle A_2(\overline{a^2}) \right\rangle.$$

If a certain relation is true for several tuples, it can be indicated in the following way:

$$\left\langle A_1(\overline{a^1}, \overline{a^2}) \right\rangle \triangleright \left\langle A_2(\overline{a^1}, \overline{a^2}) \right\rangle.$$

If a relation is established for all tuples, it can be declared as follows:

$$\langle A_1 \rangle = \langle A_2 \rangle.$$

Let us give several examples. At first, we consider two aggregates A_1, A_2 such as $A_1 \doteqdot A_2$:

$$A_1 = [\![M_1, M_2, M_3 \mid \langle 3,4,8,9 \rangle, \langle 3,1,16,12 \rangle, \langle 48,13 \rangle]\!],$$
$$A_2 = [\![M_1, M_2, M_3 \mid \langle 1,5,7,8 \rangle, \langle 8,10,11,12 \rangle, \langle 12,15 \rangle]\!].$$

The following relations can be established between these aggregates:

$$\{A_1\} \equiv \{A_2\}; \ \langle A_1 \rangle \sim \langle A_2 \rangle; \ \left\langle A_1(\overline{a^1}) \right\rangle \gg \left\langle A_2(\overline{a^1}) \right\rangle.$$

Next, let us consider two aggregates A_3, A_4 ($A_3 \doteq A_4$):

$$A_1 = [\![M_1, M_2 \mid \langle 8,10,11,12 \rangle, \langle 17,31 \rangle]\!],$$
$$A_2 = [\![M_1, M_2, M_4 \mid \langle 2,4,8 \rangle, \langle 5,7,2,6,1 \rangle]\!].$$

These aggregates can be compared by using the following relations:

$$\{A_3\} \subset \{A_4\}; \ \left\langle A_3(\overline{a^1}) \right\rangle \mapsto \left\langle A_4(\overline{a^1}) \right\rangle.$$

In all examples given above we operate with integer elements, but any other data types can be handled in a similar way.

Besides both relations between aggregates and relations between their components, we consider relations between multi-images.

Definition 3. A multi-image is a non-empty aggregate such as:

$$I = [\![T, M_1, \ldots, M_N \mid \langle t_1, \ldots, t_\tau \rangle, \left\langle a_1^1, \ldots, a_{n_1}^1 \right\rangle, \ldots, \left\langle a_1^N, \ldots, a_{n_N}^N \right\rangle]\!], \quad (29)$$

where T is a set of time values; $\tau \geq n_i$, $i \in [1, \ldots, N]$.

Since a multi-image, by definition, includes a tuple of time values as the first tuple, let us formulate the following lemma.

Lemma 1. If I_1 and I_2 are multi-images, then $I_1 \doteq I_2$.

Since compatibility is a special case of quasi-compatibility, let us state Lemma 2 which follows from Lemma 1.

Lemma 2. $\exists I_1$ and $\exists I_2$ such as $I_1 \doteqdot I_2$.

These lemmas allow us to conclude that all types of relations defined in ASA can be used for any set of multi-images.

Let us employ this theoretical background for solving practical tasks.

DOI 10.15588/1607-3274-2020-1-17

4 EXPERIMENTS

Let us consider the following discrete intervals:

$$\overline{a^1} = \left\langle a_1^1, a_2^1, a_3^1 \right\rangle = \langle 1,3,4 \rangle;$$

$$\overline{a^2} = \left\langle a_1^2, a_2^2, a_3^2, a_4^2, a_5^2 \right\rangle = \langle 8,9,12,13,16 \rangle;$$

$$\overline{a^3} = \left\langle a_1^3, a_2^3, a_3^3, a_4^3 \right\rangle = \langle 1,3,5,6 \rangle;$$

$$\overline{a^4} = \left\langle a_1^4, a_2^4, a_3^4, a_4^4 \right\rangle = \langle 8,10,14,16 \rangle;$$

$$\overline{a^5} = \left\langle a_1^5, a_2^5, a_3^5, a_4^5, a_5^5, a_6^5 \right\rangle = \langle 2,4,5,6,7,8 \rangle;$$

$$\overline{a^6} = \left\langle a_1^6, a_2^6, a_3^6 \right\rangle = \langle 6,8,10 \rangle;$$

$$\overline{a^7} = \left\langle a_1^7, a_2^7, a_3^7, a_4^7, a_5^7 \right\rangle = \langle 5,7,10,15,18 \rangle;$$

$$\overline{a^8} = \left\langle a_1^8, a_2^8, a_3^8, a_4^8 \right\rangle = \langle 8,10,11,12 \rangle;$$

$$\overline{a^9} = \left\langle a_1^9, a_2^9, a_3^9, a_4^9, a_5^9 \right\rangle = \langle 5,7,12,15,16 \rangle;$$

$$\overline{a^{10}} = \left\langle a_1^{10}, a_2^{10}, a_3^{10} \right\rangle = \langle 4,7,8 \rangle.$$

Then, we can establish the fact of the following interval relations between these tuples (Fig. 1):

$$\overline{a^1} \leftarrow \overline{a^2};\ \overline{a^2} \rightarrow \overline{a^3};\ \overline{a^2} \leftrightarrow \overline{a^4};\ \overline{a^5} \leftarrow \overline{a^2};$$

$$\overline{a^4} \mapsto \overline{a^5};\ \overline{a^3} \hookleftarrow \overline{a^5};\ \overline{a^5} \hookrightarrow \overline{a^6};\ \overline{a^6} \curvearrowleft \overline{a^7};$$

$$\overline{a^7} \curvearrowright \overline{a^2};\ \overline{a^1} \leftarrowtail \overline{a^3};\ \overline{a^2} \rightarrowtail \overline{a^8};\ \overline{a^4} \leftrightarrow \overline{a^9};\ \overline{a^5} \leftrightarrow \overline{a^{10}}.$$

Now let us solve the task related to health care. There are two patients whose health status was being monitored during a month by using several digital sensors: thermometer, pulsometer, and sphygmomanometer.

Four parameters, namely, temperature, pulse rate, systolic pressure and diastolic pressure values were being measured in the first patient and only two parameters (temperature and pulse rate) were being measured for the second patient.As a result of the monitoring, several data sequences have been obtained and composed as two multi-images: by one multi-image for each patient.

Our task is to compare these multi-images in order to let doctors conclude on comparative health status of two patients.

The data obtained from sensors belong to the following data sets:

$M_t = [35.0,\ldots,39.9]$ is a set of temperature values (°C);

$M_p = [50,\ldots,110]$ is a set of pulse values (bpm);

$M_{sp} = [80,\ldots,190]$ is a set of systolic pressure values (mmHg);

$M_{dp} = [55,\ldots,100]$ is a set of diastolic pressure values (mmHg).

There is also $T = [1, \ldots, 31]$ which is a set of time values (days of a month).

Let the data collected from sensors during the monitoring process of the first patient's health status be as follows:

$$\overline{t^1} = \langle 2,3,7,11,14,20 \rangle;$$

$$\overline{d_t^1} = \langle 36.4,36.1,36.3,36.2,36.5,36.3 \rangle;$$

$$\overline{d_p^1} = \langle 75,76,74,76,75,75 \rangle;$$

$$\overline{d_{sp}^1} = \langle 185,166,175,166,171,152 \rangle;$$

$$\overline{d_{dp}^1} = \langle 66,70,70,68,71,72 \rangle.$$

Then the obtained multi-image of the first patient's health status is:

$$I_1 = [\![T, M_t, M_p, M_{sp}, M_{dp} \mid t^1, d_t^1, d_p^1, d_{sp}^1, d_{dp}^1]\!] =$$

$$= [\![T, M_t, M_p, M_{sp}, M_{dp} \mid \langle 2,3,7,11,14,20 \rangle,$$

$$\langle 36.4,36.1,36.3,36.2,36.5,36.3 \rangle, \langle 75,76,74,76,75,75 \rangle,$$

$$\langle 185,166,175,166,171,152 \rangle, \langle 66,70,70,68,71,72 \rangle]\!].$$

Also let the data collected from sensors during the monitoring process of the second patient's health status be as follows:

$$\overline{t^2} = \langle 2,7,12,16,20 \rangle;$$

$$\overline{d_t^2} = \langle 36.8,36.6,36.3,36.4,37.0 \rangle;$$

$$\overline{d_p^2} = \langle 72,81,76,93,97 \rangle.$$

Then the obtained multi-image of the second patient's health status is as follows:

$$I_2 = [\![T, M_t, M_p \mid t^2, d_t^2, d_p^2]\!] =$$

$$= [\![T, M_t, M_p \mid \langle 2,7,12,16,20 \rangle]\!] =$$

$$= [\![\langle 36.8,36.6,36.3,36.4,37.0 \rangle, \langle 72,81,76,93,97 \rangle]\!].$$

5 RESULTS

We can establish the following relations between these multi-images:

$$\{I_1\} \supset \{I_2\}, \tag{30}$$

$$\left\langle I_1(\bar{t}) \right\rangle \leftrightarrow \left\langle I_2(\bar{t}) \right\rangle, \tag{31}$$

$$I_1 \triangleright I_2, \tag{32}$$

$$\left\langle I_1(\overline{a_t}) \right\rangle \ll \left\langle I_2(\overline{a_t}) \right\rangle, \tag{33}$$

$$\left\langle I_1(\uparrow \overline{a_p}) \right\rangle \hookrightarrow \left\langle I_2(\uparrow \overline{a_p}) \right\rangle. \tag{34}$$

DOI 10.15588/1607-3274-2020-1-17

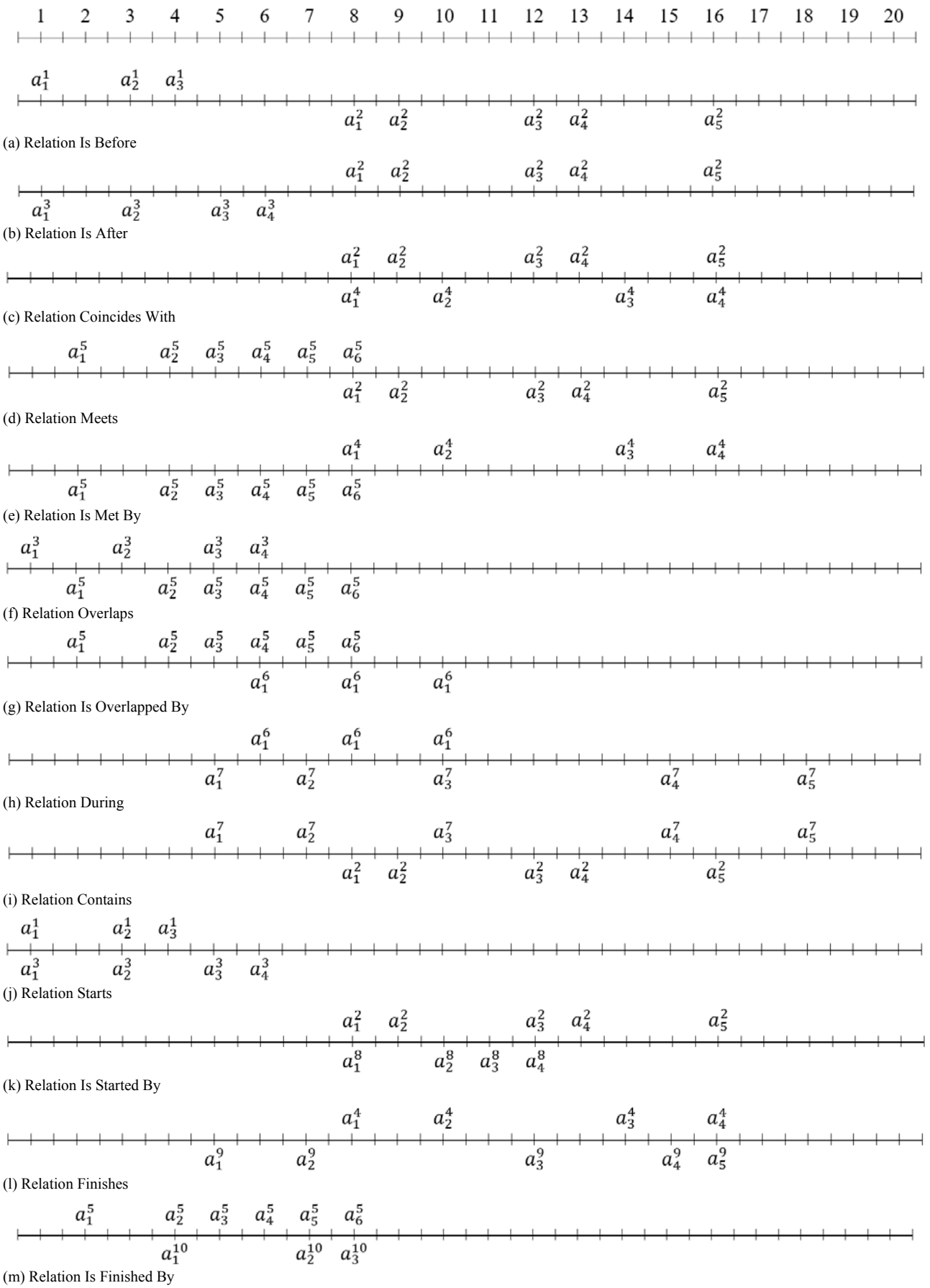


Figure 1 – Relations between discrete intervals

DOI 10.15588/1607-3274-2020-1-17

The relations (30), (31), and (32) give general comparation of multi-images and allow us to conclude that some of measurements in both aggregates belong to the same data sets and, therefore, they can be compared ($\{I_1\} \supset \{I_2\}$); data have been measured at the same period of time ($\langle I_1(\bar{t})\rangle \leftrightarrow \langle I_2(\bar{t})\rangle$); the first multi-image provides us with large amount of data ($I_1 \triangleright I_2$).

The relations (33) and (34) enable comparison of patients' health status: in most cases the second patient had higher temperature ($\langle I_1(\overline{a_t})\rangle \ll \langle I_2(\overline{a_t})\rangle$); the heart rate of the first patient was more stable because spread of values is less in the corresponding tuple of the first multi-image ($\langle I_1(\uparrow \overline{a_p})\rangle \hookrightarrow \langle I_2(\uparrow \overline{a_p})\rangle$, where ↑ means that each tuple has been sorted in ascending order [5] before interval comparison).

These relations are supposed to be applied to logical rules used in data analysis software which can be developed by employing a domain-specific programming language such as ASAMPL [6].

6 DISCUSSION

The proposed theoretical approach has been realized for multimodal data processing by using programming language ASAMPL. The experiments showed that the proposed approach of timewise aggregated data processing enables considerable decreasing of the code size (Fig. 2).

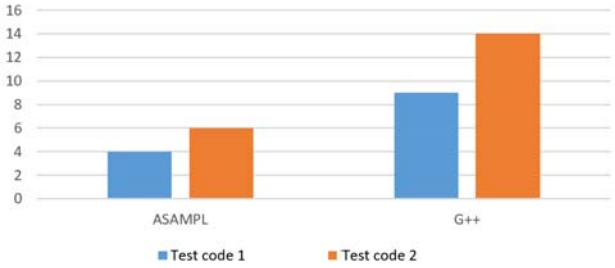


Figure 2 – ASAMPL program code comparison

To allow the work with program code in ASAMPL, the software tools for ASAMPL program code compilation and execution have been developed. They include the complier [15] and the integrated development environment (IDE) [16]. The developed ASAMPL compiler enables lexical analysis, parsing, and interpretation of the program code. The compiler is interconnected with the IDE. The developed ASAMPL IDE allows a programmer to develop code in programming language ASAMPL and debug it by analyzing the syntax errors. The developed IDE simplifies the work on a program code development by allowing the user to edit it in the full-fledged text editor with the functions of automatic code completion, color highlighting of key words, compiling and running developed programs. Fig. 3 shows the program code analysis and compilation process in ASAMPL IDE.

CONCLUSIONS

The Algebraic System of Aggregates provides the theoretical background for timewise multimodal data processing. In particular, it defines relations between tuple elements, tuples, and aggregates. This set of relations enables wide range of algorithms of processing the complex data structures such as multi-images.

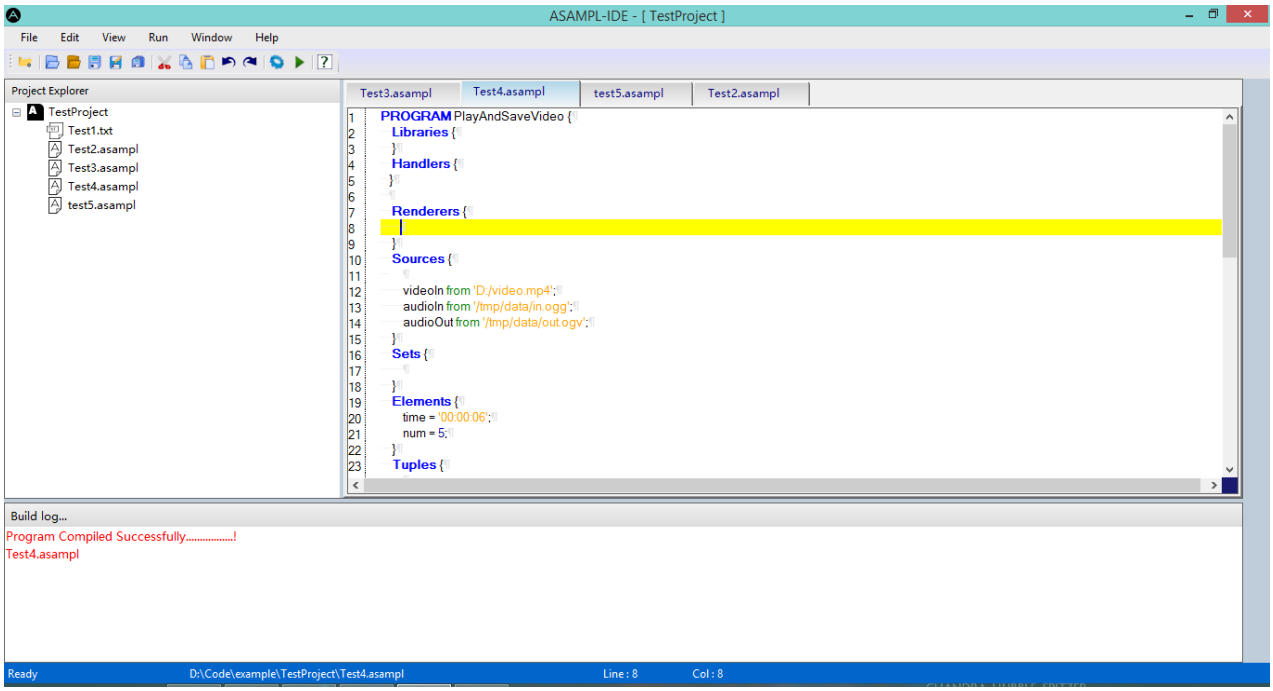


Figure 3 – ASAMPL program code in the IDE

DOI 10.15588/1607-3274-2020-1-17

A multi-image is a complex representation of multiple data sets describing an object (subject, process) of observation which are obtained (measured, generated, recorded) in the course of time. Thus, the relations defined in ASA enable processing of complex data structures presented as multi-images in data modelling, prediction and other tasks.

To allow data processing with respect to time scale, discrete intervals can be employed. A discrete interval is a tuple of time values. In the paper, we show how relations for discrete intervals comparison can be used for solving practical tasks. Besides, we present the software tools which can be used for practical implementation of the given theoretical approach by employing the domain-specific language ASAMPL.

The scientific novelty of the obtained results consists in the development of a new mathematical approach to timewise multimodal data processing which differs from the theory of sets by both including the feature of ordering and introducing new relations between elements, tuples, and complex mathematical structures called aggregates.

The practical significance of the proposed approach consists in simplification of timewise multimodal data processing and minimisation of requirements to computing resources.

Prospects for further research are to develop methods and algorithms of multimodal data processing based on ASA, including methods and algorithms of dynamic synchronization and aggregation.

ACKNOWLEDGEMENTS

The work was carried out within the framework of the research scientific work "Development and Study of Methods of Medical Images Processing, Recognition, Protection and Storing in Distributed Computer Systems" (Reg. № 0117U004267) at the Computer Systems Software Department of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

REFERENCES

1. Alakbarov R. G., Pashaev F. H., Hashimov M. A. Development of the Model of Dynamic Storage Distribution in Data Processing Centers, *International Journal of Information Technology and Computer Science*, 2015, Vol. 7, No. 5, pp. 18–24.
2. Kubiak I. The Unwanted Emission Signals in the Context of the Reconstruct Possibility of Data Graphics, *International Journal of Image, Graphics and Signal Processing*, 2014, Vol. 6, No. 11, pp. 1–9.
3. Dutta P. K., Mishra O. P., Naskar M. K. Improving Situational Awareness for Precursory Data Classification using Attribute Rough Set Reduction Approach, *International Journal of Information Technology and Computer Science*, 2013, Vol. 5, No. 12, pp. 47–55.
4. Dychka I., Sulema Ye. Logical Operations in Algebraic System of Aggregates for Multimodal Data Representation and Processing, *KPI Science News*, 2018, Vol. 6, pp. 44–52.
5. Dychka I., Sulema Ye. Ordering Operations in Algebraic System of Aggregates for Multi-Image Data Processing, *KPI Science News*, 2019, Vol. 1, pp. 15–23.
6. Sulema Ye. ASAMPL: Programming Language for Mulsemedia Data Processing Based on Algebraic System of Aggregates, *Advances in Intelligent Systems and Computing*, Springer, 2018, Vol. 725, pp. 431–442.
7. Allen J. F. Maintaining knowledge about temporal intervals, *Communications of ACM*, 1983, pp. 832–843.
8. Allen J. F., Hayes P. J. Moments and points in an interval-based temporal logic, *Computational Intelligence*, 1989, Vol. 5, Issue 3, pp. 225–238.
9. Nebel B., Bürckert H.-J., Reasoning About Temporal Relations: A Maximal Tractable Subclass of Allen's Interval Algebra, *Journal of the Association for Computing Machinery*, 1995, Vol. 42, No. 1, pp. 43–66.
10. Allen J. F., Ferguson G. Actions and Events in Interval Temporal Logic, *Spatial and Temporal Reasoning*, Springer, 1997, Part 3, pp. 205–245.
11. Schockaert S., De Cock M., Kerre E., Reasoning About Fuzzy Temporal and Spatial Information from the Web, *Intelligent Information Systems*, 2010, Vol. 3, 608 p.
12. Bozzelli L., Molinari A., Montanari A. et al. Interval vs. Point Temporal Logic Model Checking: an Expressiveness Comparison, *ACM Transactions on Computational Logic*, 2018, Vol. 20, № 1, Article № 4, 31 p.
13. Grüninger M., Li Zh., The Time Ontology of Allen's Interval Algebra, *Proceedings of 24th International Symposium on Temporal Representation and Reasoning* (TIME 2017), Mons, 16–18 October 2017, Article No. 16, pp. 16:1–16:16.
14. Fraenkel A. A., Bar-Hillel Y., Levy A. Foundations of Set Theory, *Studies in Logic and the Foundations of Mathematics*. Elsevier, 1973, Vol. 67, 415 p.
15. Peschanskii V. Yu. ASAMPL compiler, Thesis of Bachelor in Software Engineering. Kyiv, Igor Sikorsky KPI, 2019, 110 p.
16. Krysiuk A. M. ASAMPL IDE, Thesis of Bachelor in Software Engineering. Kyiv, *Igor Sikorsky KPI*, 2019, 108 p.

Received 27.12.2019.
Accepted 06.02.2020.

УДК 004.6

ОБРОБЛЕННЯ МУЛЬТИМОДАЛЬНИХ ДАНИХ ЗА ДОПОМОГОЮ ВІДНОШЕНЬ АЛГЕБРАЇЧНОЇ СИСТЕМИ АГРЕГАТІВ

Сулема Є.С. – канд. техн. наук, доцент кафедри програмного забезпечення комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

АНОТАЦІЯ

Актуальність. В багатьох інженерних задачах, пов'язаних з необхідністю моніторингу змін характеристик об'єкта, суб'єкта або процесу спостереження, є потреба у обробленні мультимодальних даних, що реєструються зі встановленням моменту часу їх вимірювання. У цій статті автор представляє новий підхід до вирішення задачі часового оброблення структур мультимодальних даних, який дозволяє спростити оброблення таких даних за рахунок використання математичного апарата алгебраїчної системи агрегатів й тим самим зменшити вимоги, що висуваються до обчислювальних ресурсів. Алге-

DOI 10.15588/1607-3274-2020-1-17

браїчна система агрегатів оперує такими специфічними структурами даних як агрегати, мультиобрази та дискретні інтервали. Метою цієї роботи є формалізація відношень меж базовими математичними об'єктами, що визначені в алгебраїчній системі агрегатів, а саме, елементами, кортежами та агрегатами, а також структурами даних, які ґрунтуються на цих математичних об'єктах, а саме, дискретними інтервалами та мультиобразами, що дозволить виконувати ефективне оброблення мультимодальних даних, що визначені з урахуванням часу їх реєстрації.

Метод. Дослідження, результати якого представлені у цій статті, ґрунтується на використанні основних положень алгебраїчної системи агрегатів та концепції мультиобразу, які дозволяють спростити оброблення структур мультимодальних даних, що визначені у часі. Носієм алгебраїчної системи агрегатів є множина структур даних, що називають агрегатами. Агрегат являє собою кортеж кортежів, елементи яких належать наперед визначеним множинам. В алгебраїчній системі агрегатів визначені логічні операції, операції впорядкування та арифметичні операції над агрегатами. Мультиобразом називають непорожній агрегат, перший кортеж якого є кортежом значень часу. Такий кортеж часових міток являє собою дискретний інтервал. Для оброблення дискретних інтервалів та мультиобразів в алгебраїчній системі агрегатів визначено множину відношень. Ця множина включає відношення між елементами кортежів, відношення між кортежами та відношення між агрегатами. Зокрема, відношення між кортежами дозволяють виконувати арифметичне порівняння, частотне порівняння та інтервальне порівняння. Математичний апарат алгебраїчної системи агрегатів може використовуватись як для комплексного подання мультимодальних характеристик об'єкта (суб'єкта, процесу) дослідження, так і для подальшого оброблення цих даних, зв'язаних з часовими мітками і поданих у вигляді мультиобразу.

Результати. У статті розроблено та представлено новий підхід до оброблення мультимодальних даних, зокрема, дискретних інтервалів та мультиобразів, який ґрунтується на відношеннях, що визначені в алгебраїчній системі агрегатів. Наведено приклади практичного застосування розробленого підходу.

Висновки. Результати, що отримані у цьому досліджені, дозволяють зробити висновок про те, що відношення, які визначені в алгебраїчній системі агрегатів, можуть бути застосовані для оброблення складних структур даних, що мають назву мультиобрази, в задачах аналізу даних, моделювання, прогнозування тощо. Для оброблення даних, що визначені у прив'язці до деякої шкали часу, можуть застосовуватись цифрові інтервали. У статте автор демонструє, як відношення для порівняння цифрових інтервалів можуть використовуватись для вирішення практичних задач. Крім того, автор представляє програмні інструменти, які можуть бути застосовані для практичної реалізації запропонованого теоретичного підходу з використанням спеціалізованої мови програмування ASAMPL.

КЛЮЧОВІ СЛОВА: оброблення мультимодальних даних, агрегат, мультиобраз, дискретний інтервал.

УДК 004.6

ОБРАБОТКА МУЛЬТИМОДАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ОТНОШЕНИЙ АЛГЕБРАИЧЕСКОЙ СИСТЕМЫ АГРЕГАТОВ

Сулема Е. С. – канд. техн. наук, доцент кафедры программного обеспечения компьютерных систем Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», Киев, Украина.

АННОТАЦИЯ

Актуальность. Во многих инженерных задачах, связанных с необходимостью мониторинга изменений характеристик объекта, субъекта или процесса наблюдения, требуется осуществлять обработку мультимодальных данных, регистрируемых с установлением момента времени их измерения. В данной статье автор представляет новый подход к решению задачи временной обработки структур мультимодальных данных, который позволяет упростить обработку таких данных за счет использования математического аппарата алгебраической системы агрегатов и тем самым уменьшить требования, предъявляемые к вычислительным ресурсам. Алгебраическая система агрегатов оперирует такими специфическими структурами данных как агрегаты, мультиобразы и дискретные интервалы. Целью данной работы является формализация отношений между базовыми математическими объектами, определенными в алгебраической системе агрегатов, такими как элементы, кортежи и агрегаты, а также структурами данных, основанными на этих математических объектах, а именно дискретными интервалами и мультиобразами, что позволит осуществлять эффективную обработку мультимодальных данных, определенных с учетом времени их регистрации.

Метод. Исследование, результаты которого представлены в данной статье, основано на использовании основных положений алгебраической системы агрегатов и концепции мультиобраза, которые упрощают обработку мультимодальных данных, представленных во времени. Носителем алгебраической системы агрегатов является множество структур данных, называемых агрегатами. Агрегат представляет собой кортеж кортежей, элементы которых принадлежат предопределенным множествам. В алгебраической системе агрегатов определены логические операции, операции упорядочения и арифметические операции над агрегатами. Мультиобразом называется непустой агрегат, первый кортеж которого является кортежем значений времени. Такой кортеж временных меток представляет собой дискретный интервал. Для обработки дискретных интервалов и мультиобразов в алгебраической системе агрегатов определено множество отношений. Это множество включает отношения между элементами кортежей, отношения между кортежами и отношения между агрегатами. В частности, отношения между кортежами позволяют осуществлять арифметическое сравнение, частотное сравнение и интервальное сравнение. Этот математический аппарат может использоваться как для комплексного представления мультимодальных характеристик объекта (субъекта, процесса) исследования, так и последующей обработки этих данных, связанных со временными метками и представленных в виде мультиобраза.

Результаты. В статье разработан и представлен новый подход к обработке мультимодальных данных, в частности, дискретных интервалов и мультиобразов, основанный на отношениях, которые определены в алгебраической системе агрегатов. Приведены примеры практического использования разработанного подхода.

DOI 10.15588/1607-3274-2020-1-17

Выводы. Результаты, полученные в данном исследовании, позволяют сделать вывод о том, что отношения, определенные в алгебраической системе агрегатов, могут быть использованы для обработки сложных структур данных, называемыми мультиобразами, в задачах анализа данных, моделирования, прогнозирования и других. Для обработки данных, определенных в привязке к некоторой шкале времени, могут использоваться цифровые интервалы. В статье автор показывает, как отношения для сравнения цифровых интервалов могут использоваться для решения практических задач. Кроме того, автор представляет программные инструменты, которые могут быть использованы для практической реализации данного теоретического подхода с использованием специализированного языка программирования ASAMPL.

КЛЮЧЕВЫЕ СЛОВА: обработка мультимодальных данных, агрегат, мультиобраз, дискретный интервал.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Alakbarov R. G. Development of the Model of Dynamic Storage Distribution in Data Processing Centers / R. G. Alakbarov, F. H. Pashaev, M. A. Hashimov // International Journal of Information Technology and Computer Science. – 2015. – Vol. 7, № 5. – P. 18–24.
2. Kubiak I. The Unwanted Emission Signals in the Context of the Reconstruct Possibility of Data Graphics / I. Kubiak // International Journal of Image, Graphics and Signal Processing. – 2014. – Vol. 6, № 11. – P. 1–9.
3. Dutta P. K. Improving Situational Awareness for Precursory Data Classification using Attribute Rough Set Reduction Approach / P. K. Dutta, O. P. Mishra, M. K. Naskar // International Journal of Information Technology and Computer Science. – 2013. – Vol. 5, № 12. – P. 47–55.
4. Dychka I. A. Logical Operations in Algebraic System of Aggregates for Multimodal Data Representation and Processing / I. A. Dychka, Ye. S. Sulema // KPI Science News. – 2018. – Vol. 6. – P. 44–52.
5. Dychka I. A. Ordering Operations in Algebraic System of Aggregates for Multi-Image Data Processing / I. A. Dychka, Ye. S. Sulema // KPI Science News. – 2019. – Vol. 1. – P. 15–23.
6. Sulema Ye. S. ASAMPL: Programming Language for Mulsemedia Data Processing Based on Algebraic System of Aggregates / Ye. S. Sulema // Advances in Intelligent Systems and Computing. – Springer, 2018. – Vol. 725. – P. 431–442.
7. Allen J. F. Maintaining knowledge about temporal intervals / J. F. Allen // Communications of ACM. – 1983. – Vol. 26, № 11. – P. 832–843.
8. Allen J. F. Moments and points in an interval-based temporal logic / J. F. Allen, P. J. Hayes // Computational Intelligence. – 1989. – Vol. 5, № 3. – P. 225–238.
9. Nebel B. Reasoning About Temporal Relations: A Maximal Tractable Subclass of Allen's Interval Algebra / B. Nebel, H.-J. Bürckert // Journal of the Association for Computing Machinery. – 1995. – Vol. 42, № 1. –P. 43–66.
10. Allen J. F. Actions and Events in Interval Temporal Logic / J. F. Allen, G. Ferguson // Spatial and Temporal Reasoning. – Springer, 1997. – Part 3. – P. 205–245.
11. Schockaert S. Reasoning About Fuzzy Temporal and Spatial Information from the Web / S. Schockaert, M. De Cock, E. Kerre // Intelligent Information Systems. – 2010. – Vol. 3. – 608 p.
12. Interval vs. Point Temporal Logic Model Checking: an Expressiveness Comparison / [L. Bozzelli, A. Molinari, A. Montanari, et al.] // ACM Transactions on Computational Logic. – 2018. – Vol. 20, № 1. – Article № 4. – 31 p.
13. Grüninger M. The Time Ontology of Allen's Interval Algebra / M. Grüninger, Zh. Li // Temporal Representation and Reasoning : 24th International Symposium, Mons, 16–18 October 2017 : proceedings. – Schloss Dagstuhl : Leibniz Center for Informatics, 2017. – Article № 16. – P. 16:1–16:16.
14. Fraenkel A. A. Foundations of Set Theory / A. A. Fraenkel, Y. Bar-Hillel, A. Levy // Studies in Logic and the Foundations of Mathematics. – Elsevier, 1973. – Vol. 67. – 415 p.
15. Peschanskii V. Yu. ASAMPL compiler : thesis … bachelor : software engineering / Peschanskii Vladyslav Yuriyovych. – Kyiv : Igor Sikorsky KPI, 2019. – 110 p.
16. Krysiuk A. M. ASAMPL IDE : thesis … bachelor : software engineering / Krysiuk Andrii Mykhaylovych. – Kyiv : Igor Sikorsky KPI, 2019. – 108 p.

DOI 10.15588/1607-3274-2020-1-17

e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2020. № 1
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2020. № 1

UDC 004.056

A METHOD OF THE TRANSMITTED BLOCKS INFORMATION INTEGRITY CONTROL

Tanygin M. O. – Dr. Sc., Associate Professor, Head of the department of Information Security, Southwest State University, Kursk, Russian Federation.

Alshaeaa H. Y. – Post-graduate student of the department of Information Security, Southwest State University, Kursk, Russian Federation.

Kuleshova E. A. – Post-graduate student of the department of Information Security, Southwest State University, Kursk, Russian Federation.

ABSTRACT

Context. For the proper operation of the hardware and software systems, it is necessary that the hardware component receives data only from the corresponding software. Otherwise, the data received from extraneous programs that can be perceived and processed by the device, which can lead to errors in the operation of the device or even a complete loss of its functionality or data.

Objective. In order to increase the reliability of legal software data and identify the challenges of the transfer of blocks, this article focuses on a comprehensive study of the problems arising from the transmission of information in the form of separate data blocks.

Method. The methods of integrity control in modes of transmission are described. The method based on hashes and block delivery time is analyzed in detail, analysis the methods of reducing the probability of errors occurring in the receiver and the possibility of reducing the reception of the extraneous blocks when receiving individual blocks of information. This is done by using a set of mathematical equations. And measure the extent of the effect of intensity of receiving extraneous blocks and hash field length.

Results. In the process of analyzing systems in which information is transmitted by block, when using the method of formation of information chains based on the method the hashes and the delivery time of the block, where we note, when the value of the hash field is equal to 6 or more, the probability of occurrence of duplicate branches is acceptably low. Where, when hash field more then 6, the parameter of length of a chain practically does not affect the final probability of constructing a chain from the extraneous blocks. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at hash field more 6 is about1 10–3, which it's acceptable for real information transmission systems.

Conclusions. Based on the analysis, we can conclude that in systems in which information is transmitted block by block, when using the method of generating information chains based on the hash and block arrival time, with a hash field of 6 or more, the probability of occurrence of duplicate branches is acceptably low.

KEYWORDS: probability calculation, messages limited in length, authentication control, hash field length, duplicating branches in a chain.

ABBREVIATIONS

FB is a foreign block;

FC is a foreign chain.

NOMENCLATURE

F_{hash} is a hash-function;

H is a length of the hash field;

K is a parameter of simulated (intensity of receiving extraneous block);

L is a length of a chain;

N is a number of block;

P_B – probability of receiving blocks from of the correct chain;

p_C is a probability of adding the first incoming foreign block to the chain;

$p(i)$ is a binomial law of the received blocks are distributed;

P_{FB} – probability of receiving the foreign block;

$p(n_{FB},l)$ – probability of obtaining the receiver exactly n_{FB} blocks during the time of obtaining l legal blocks;

S_{false} is a block from another chain;

S_{rec} is an incoming data block;

$S_{\text{rec}}^{\text{hash}}$ is a hash part of the incoming block;

S_r^{inf} is an information part of the incoming block number r.

INTRODUCTION

Technology block-chain, that integration into a structured sequence of information, which represented in the form of separate blocks due to the use of the cryptographic hashing functions, it has recently gained wide popularity.

The identification information of the received block is compared with the information processed according to rules of information from the information blocks that already received by the receiver to the present moment, and, in case of coincidence, the block is added to the sequence as shown in Figure (1).

As practice shows, the approaches used in modern blockchain systems, where the large blocks of information are structured and unacceptable for chains consisting of small size blocks, accordingly, having hashes with a length that does not allow us to talk about a negligible probability of their coincidence, as in the case of standardized algorithms for cryptographic hashing. We are talking about blocks of information that size up to several tens of bits, which are used in radio identification systems, as instructions for the program the control of devices, etc. [6].

DOI 10.15588/1607-3274-2020-1-18

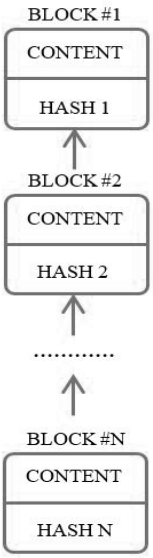


Figure 1 – Blocks that are combined into a sequence based on the identification information

The object of study is a comprehensive study of the problems arising from the transmission of information in the form of separate data blocks.

The subject of study is the methods of integrity control in modes of transmission are described. The method based on hashes and block delivery time is analyzed in detail, analysis the methods of reducing the probability of errors occurring in the receiver and the possibility of reducing the reception of the extraneous blocks when receiving individual blocks of information.

The purpose of the work is to increase the reliability of legal software data and identify the challenges of the transfer of blocks.

1 PROBLEM STATEMENT

There are many options for formation of identification data of information blocks and their analysis.

1. Only the hash of the previous blocks is used as identification data. The receiver analyzes the hashes of all received blocks and determines the location of the newly received blocks.

2. Only the hash of the previous blocks is used as identification data, but the receiver when determining the location of the block in the chain, takes account the time of its receipt. That means, if the one block arrived at the receiver later than the other, then in the formed chain it should take place with a higher index.

3. The hash of the previous blocks and the block index in the chain are used as identification data. The block index in the chain refers to uniquely positions of the block in the chain, while the hash is used exclusively to prevent extraneous blocks from entering to the chain.

Each of the described approaches has advantages and disadvantages for determining the membership of the chain block.

Based on the calculation of hashes, there is a little repetition of the information if it is compared with a method based on the calculation of hashes and the block index in the chain. The disadvantage is the complexity of determining the location of the block in the chain, because this requires comparing with the all hashes blocks in the chain. And if the chain is longer, that mean, this process will take a long time.

The disadvantage of the method based on the calculation of hashes and the delivery time of the block is the impossibility of responding this situation, when the information block issued earlier came as a result of delays later than the subsequent one. This situation is possible in telecommunication networks (wired and remote communication). In addition, the algorithm becomes more complicated to separate the blocks from several chains, in the case, when the blocks formed by several sources are transmitted through one communication channel. The advantage of this method includes the fact that the delivery time of the block itself adds more information about the block and its place in the chain. At the same time, it does not create additional redundancy information, which allows achieving the same reliability transmission characteristics as in the method based on hash functions, with a shorter length of the hash field itself.

The method of identifying the block based on the hash and the block index in the chain is the most reliable, both in terms of the reliability of the receiver separation of information blocks of different chains, and in terms of the algorithmic complexity of the formation of the block chains themselves. In the latter case, the block index determines a uniquely place in the chain [10]. But this is causing the main drawback of this method – the length of the chain is limited because the maximum size which is determined by the bit width of the index field. In addition, we obtain additional information redundancy, since instead of a probabilistic approach to determining the place of a block in chains by its hash (which means losing some of the information, and hence a decrease in the length of additional fields) we have a strictly defined index value [11, 12].

Let's consider in more detail one of the methods – based on hashes and block delivery time. The incoming data block S_{rec} consists of the information part $S_{\text{rec}}^{\text{inf}}$ and the hash result $S_{\text{rec}}^{\text{hash}}$, that obtained from the data of the previous block of the chain [13, 14]:

$$S_{\text{rec}} = \left\{ S_{\text{rec}}^{\text{inf}} \mid S_{\text{rec}}^{\text{hash}} \right\}. \quad (1)$$

If the hash, calculated from block number *r*, the last chain block at the current moment, coincides with the hash $S_{\text{rec}}^{\text{hash}}$, then the block S_{rec} will be added to the chain and becomes the last one:

$$S_{\text{rec}}^{\text{hash}} = F_{\text{hash}}\left(S_r^{\text{inf}}\right) \quad (2)$$

It is natural, with this approach raises the issue of collisions. If a block from another chain S_{false} (while we do

DOI 10.15588/1607-3274-2020-1-18

not consider how it was formed as a result of the actions of intruders or because availability of several sources of chain formation) arrives to the receiver, and its hash matches with the hash that obtained from the last block of the current chain:

$$S_{\text{false}}^{\text{hash}} = F_{\text{hash}}\left(S_r^{\text{inf}}\right), \quad (3)$$

this "extraneous" block will be added to the chain as block number r+1, and the "correct" block number r+1 that comes after it will be ignored because of the mismatch of its own hash with another hash, that obtained from the data of the "extraneous" block:

$$S_{\text{r+1}}^{\text{hash}} \neq F_{\text{hash}}\left(S_{\text{false}}^{\text{inf}}\right) \quad (4)$$

To prevent this situation, it is necessary to compare the hash of the received block not only with the hash from the last block of the chain, but also with all hashes that obtained from all the blocks that make up the chain until the present moment. Let a_{j+1} is a number of words, received in the receiver, the hash of which coincided with the hash formed from the j-th word in the chain:

$$\begin{aligned} &S_{j,a_j} = S_{\text{rec}}, a_j = a_j + 1, \\ &\text{if } S_{\text{rec}}^{\text{hash}} = F_{\text{hash}}\left(S_j^{\text{inf}}\right), \; j = \overline{1,r}. \end{aligned} \quad (5)$$

But as a result, the chain of blocks is processed by the receiver and transformed into a tree, as shown in Figure (2), where the numbers refer to the block numbers in the corresponding chain, and the number in bracket refer to the branch number of the block in the block tree.

In addition to the complexity of storing that similar to the tree structure, like this approach leads to a number of problems that we will be considered below.

The problem of duplicating branches in a chain occurs when the hash of the received block coincides not only with the hash of the last block of the chain, but also with a hash that obtained from one of the earlier blocks. As a result of this situation, when receiving subsequent blocks, they will be attributed not only of the main chain as shown in the figure (2), but also to the secondary, since their hashes will completely satisfy the inclusion condition both one, and another branch of the chain.

There are three methods to resolve this problem. The first method is to choose the longest chain from all the possible branches of the chain.

The second method involves changing the format of the blocks, where there is one hash from several consecutive blocks of a chain that controls on the sequence of these blocks. This would reduce, though not completely exclude, the possibility of the formation of such side branches in the chain [15, 16].

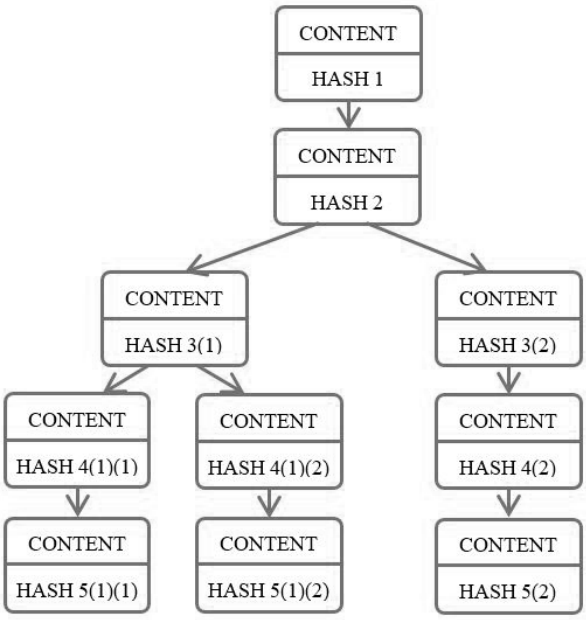


Figure 2 – Block tree, arising as a result of the coincidence of the hash of the received block with the hash of the last block in the chain

The third method is to periodically check the length of all the chains and cutting those that do not correspond to the threshold conditions. For example, the length of the chain is less than the length of the maximum chain by a fixed value L. In this case, we allow the erroneous to the removal of the correct chain. The present work is devoted to the consideration of this method and the study of its characteristics.

In system where the positioning of the block is carried out exclusively by matching the hash of the current block, the probability of duplicate chains is determined only by the hash field length H in bits. In turn, the probability of incorrect selection of chains depends on the value of L – the difference between the length of the longest chain in the tree and the shortest one that has not yet been cut off. Below we describe a method that allows you to determine the relationship between these two parameters and the probability of erroneous deletion of the correct chain.

2 REVIEW OF THE LITERATURE

At the same time, similar approaches have been used earlier to authentication of two subjects of exchange information [1–3]. The principle of interaction between the source (the generator of information blocks) and the receiver (recipient of information blocks) is based on the fact that identification information generated in some way is added to a block and usually add a hash of one or several previous information blocks, which allows to accurately determine, firstly, the identity of the specific sequence of the information block, secondly, the place of the block in sequence.

Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. This iterative process confirms the integrity of

DOI 10.15588/1607-3274-2020-1-18

the previous block, all the way back to the original genesis block. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in any block, will change the hash which is stored before this block and so on and so forth [4, 5]. This will completely change the chain, which is impossible.

With the rapid development of transfer blocks technology, different industries gradually realize technological superiority. In the meantime, there are still some technical challenges and limitations in mass transfer technologies and data to the real source. A good example for this is the problems and security risks in blockchain application are becoming more and more obvious, such as 51% attack [7] and limited size of block [8]. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any transfer blocks technology has a specified algorithm for scoring different versions of the history so that one with a higher value can be selected over others. In order to identify the challenges of the transfer of blocks, this paper is a comprehensive study of the problems that arise from the use of the method the hashes and the delivery time of the block and the possibility of reducing the reception of extraneous blocks [9].

The problem of embedding the extraneous block in a chain occurs when the one or several blocks of extraneous chains fall into the gap between two adjacent blocks of the chain, the hashes of which satisfy the condition of their inclusion in the chain. As a result, the chain extends over these several extraneous blocks. If, by analogy with the problem of duplicating chains, compare the hash of the incoming block not only with the hash from the last block of the chain, but also with all hashes that obtained from all the blocks included in the chain until the present moment, then we get a tree in which the longest chain is a chain with extraneous blocks. The correct chain is shorter than the maximum chain by one or more blocks. Accordingly, of the methods described above to counter the formation of erroneous chains, the only acceptable can only be the control of individual consecutive blocks by using an additional hash field [17, 18].

3 MATERIALS AND METHODS

To find the dependence between values L and H and the probability of incorrect chain clipping, we apply the same mathematical model as in [19]. Let's imagine the process of receiving information blocks by the receiver (both blocks of the correct chain, and the extraneous blocks – blocks of other chains and random blocks that received by the receiver) as a random Poisson process, this a process without a background in which the probability of obtaining the next block does not depend on how much the period that blocks were received before it. Let the intensity of obtaining extraneous blocks K times more than the intensity of the formation of blocks of the legal or correct chain:

$$P_{FB} = K \times P_B. \quad (6)$$

Since we are using a method based on the elimination of those chains that are less than the maximum by any number L, it's logical to check the hash of each newly obtained block for a match with the hashes of not all blocks and branches of the chain, but only with those that belong to the branches that depart from the last L blocks of the longest chain to the present moment. To do this we assume that the longest chain to the beginning of the simulation consists entirely of legal blocks and the number of these blocks is N.

Let in this time, during the receiver receives l blocks, the number of extraneous blocks will be n_{FB}. This number will be distributed according to the Poisson law with the expectation $K \times l$:

$$p(n_{FB}, l) = \frac{(K \cdot l)^{n_{FB}} \times e^{-(K \cdot l)}}{n_{FB}!}. \quad (7)$$

The probability of adding a block to any chain is determined by the width of the hash field: $p_C = 2^{-H}$, where H – is the length of the hash field in bits.

Next, we will implement the following reasoning. Each block comes independently of the other and can be simultaneously added to the several branches. If we consider a specific block, the first incoming foreign block will be added to the chain after it with probability p_C, and ignored with probability $(1 - p_C)$. For the second and third block that came, the probabilities are similar. The probability of forming a chain of three blocks will be $(p_C)^3$, the probability of forming a chain of two blocks will be the sum of three terms:

– $p_C \times p_C \times (1 - p_C)$ – The probability that the first two blocks are added and the third is ignored.

– $p_C \times (1 - p_C) \times p_C$ – The probability that the first and third blocks will be added and the second is ignored.

– $(1 - p_C) \times p_C \times p_C$ – The probability that the second and third blocks will be added and the first is ignored.

The probability of forming a chain from one block will also be equal to the sum of three terms:

– $p_C \times (1 - p_C) \times (1 - p_C)$ – probability that the first block will be added,

– $(1 - p_C) \times p_C \times (1 - p_C)$ – probability that the second block will be added,

– $(1 - p_C) \times (1 - p_C) \times p_C$ – probability that the third block will be added.

The probability of ignoring all the blocks (the construction of length a chain is zero) will be $(1 - p_C)^3$. Similar reasoning can be carried out for an arbitrary number of extraneous blocks. It can be seen, the probability of adding to an arbitrary block of a branched chain of length i of blocks from n_{FB} of the received blocks are distributed according to the binomial law:

$$p(i) = C^i_{n_{FB}} \cdot (p_C)^i \cdot (1 - p_C)^{n_{FB-i}}. \quad (8)$$

DOI 10.15588/1607-3274-2020-1-18

Let us define the probability p_{FC} of constructing a chain from the extraneous blocks, where length longer than the number of legal blocks. This will happen in the event that during the time during which the receiver receives and writes a new block to the chain, from the block under the number N will be built a branch not less than 2 extraneous blocks, from the block under the number $N-1$ will be built a branch not less than 3 extraneous blocks, etc., up to the block under the number ($N–L$ + 1), from the length of a chain (L+ 2) and more should be constructed as shown in Figure (3).

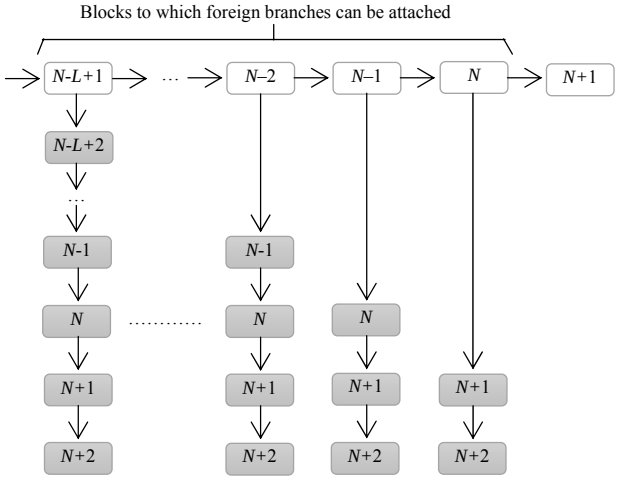


Figure 3 – Building a chai that length is longer than number of legal blocks

Since all branches consisting of their extraneous blocks (in the figure shows hatching), are being built independent of each other and in the general case can consist of the same blocks, the probabilities of their construction are independent of each other. Then probability of finding the number of extraneous blocks in n_{FB} will be defined as:

$$p(n_{FB}) = \sum_{i=1}^{L} \left\{ \sum_{j=1+i}^{n_{FB}} C_{n_{FB}}^{j} \cdot (p_C)^j \cdot (1-p_C)^{n_{FB}-j} \right\}. \quad (9)$$

In common case, combining the received expression with the formula for $p(n_{FB}, l)$ at l=1:

$$p_{FC} = \sum_{v=2}^{\infty} \left\{ \frac{K^v \times e^{-K}}{v!} \times \sum_{i=1}^{L} \left[\sum_{j=1+i}^{v} C_v^i \cdot (p_C)^j \cdot (1-p_C)^{v-j} \right] \right\}, \quad (10)$$

$$v \geq i+1.$$

4 EXPERIMENTS

In Figure (4) are presented graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the intensity of receiving extraneous blocks K and the length of the hash field H in bits and the number of blocks L which extraneous blocks can be attached.

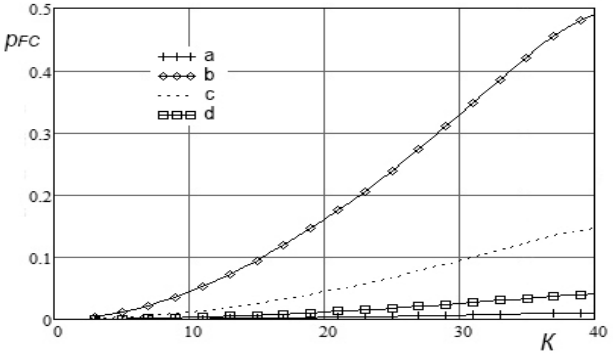


Figure 4 – the graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the intensity of receiving extraneous blocks K and the length of the hash field H in bits with L =4.
a) H = 5; b) H = 6; c) H = 7; d) H = 8

Calculations show the number of blocks L which blocks can be joined by extraneous blocks, does not effect on the probability of constructing a long chain from extraneous blocks.

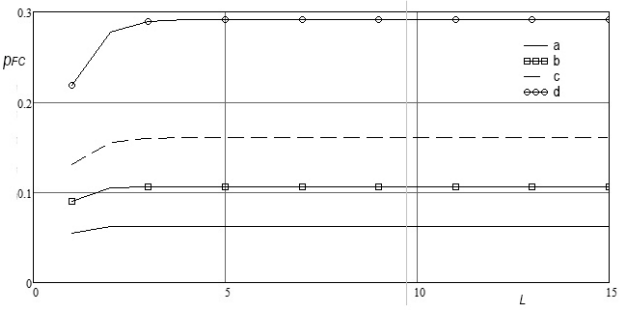


Figure 5 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, from the parameter L and the intensity of receiving extraneous blocks K for a fixed hash field length H = 4.
a) K = 3; b) K = 4; c) K = 5, d) K=7

This is easily explained by the fact that the probability of constructing long chains of extraneous blocks is negligible, if compared with the probability of constructing branches with a length of one or two blocks. like this chains can be lead to the error of determining the longest chain that only starting from the last (the penultimate legal block of a chain).This is clearly to seen in the figure (5), where the graphs dependence of p_{FC} on L that represent a practically horizontal straight line starting with the values L = 3 ... 5.

5 RESULTS

Based on the graphs received, we can conclude what contribution to the final probability of the p_{FC} that make certain of its components. It can be seen that depending on the value intensity of receiving extraneous blocks K, the sum of the probabilities of constructing side chains that are more than legal blocks length, from the last 2 is

DOI 10.15588/1607-3274-2020-1-18

from 80% to 95% of the total probability of constructing side chains from all L last blocks. For the sum of probabilities for the last 4 blocks, this is increases to 98% – 99.9%. These values will be useful to us in the future, when modeling of the receiver by the receiver of more than one legal of block or in the situations, when the time of obtaining the last legal block by the receiver is already available, in addition to the main a number of side chains.

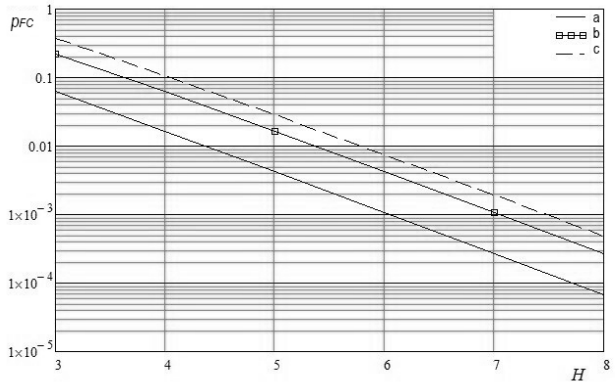


Figure 6 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the length of the hash field H and the intensity of receiving extraneous blocks K with $L = 5$.
a) $K = 3$; b) $K = 6$; c) $K = 8$

Finally, we explore the impact length of the hash field on the probability of constructing a long chain of extraneous blocks. In Figure (6) shows this dependence for greater clarity on a logarithmic scale. It can be seen this is practically an exponential dependence of the form $p_{\text{FC}} = k1 \times e^{-k2 \cdot H}$.

As an intermediate result, we can say that there is no great need to increase the parameter L – the number of blocks to which incoming blocks can be attached. If there are no additional conditions, it can be selected in the range from 3 to 6, varying only the length of the hash field during transmission, that depending on the observed intensity of receiving extraneous blocks. This parameter can be calculated dynamically as a ratio of the number of information blocks that received during a certain period, to the maximum lengthening for the same period of the longest chain [19].

Next, we simulate the interval during the receiver received more than one legal block. To do this, consider the chains that were formed at the time of obtaining N blocks (Figure (7)). In addition to the main chain, the chain V^N – V^{N-L+2} to which the resulting blocks can be attached. This is due to the fact that the chain V^{N-L+1} it will be impossible to join the blocks because to the above limitations. Also, based on the results that obtained above, we can say that the probability the length of the chain V^{N-L+1} will exceed the number L is negligible if compared with the total probability p_{FC} (Depending on the length of the field, were the values from $10^{-12}$to 10^{-8}).

Strictly speaking, each chain like this will be representing a bush the chains of arbitrary length.

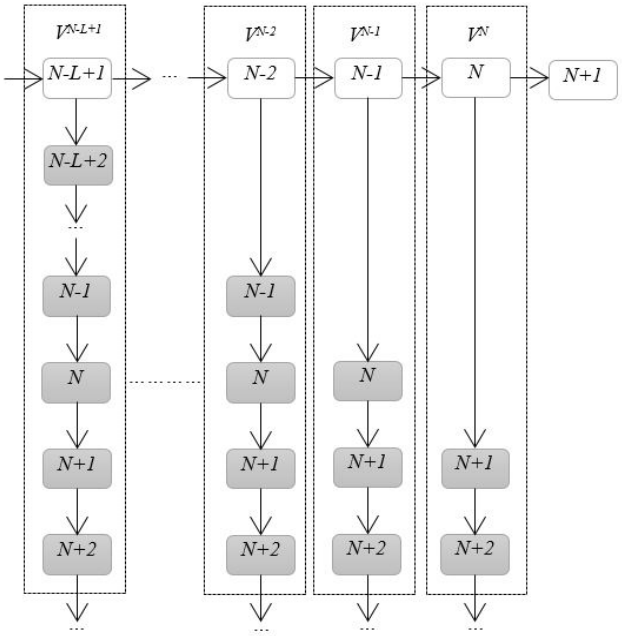


Figure 7 – The chains formed to the moment of obtaining N+1 legal block

Now we must take into account, that the chain V^N is formed from the extraneous blocks that obtained by the receiver between obtaining N and N+1 blocks, the chain V^{N-1} is formed from extraneous blocks that obtained by the receiver between obtaining N–1 and N+1 blocks, the chain V^{N-2} is formed from extraneous blocks that obtained by the receiver between obtaining N–2 and N+1 blocks, etc. Accordingly, the final probability of constructing a complex chain exceeding the main length, that determined by the sum of the probabilities of constructing chains V^N – V^{N-L+2} corresponding lengths. For a chain with the number V^{N-i} it is equal to (i +2).

For a chain V^{N-i}, by analogies with formula (5), the expression takes the form:

$$p_{V^{N-i}} = \sum_{v=i+2}^{\infty} \frac{((i+1)\times K)^v \times e^{-((i+1)\times K)}}{v!} \sum_{j=v}^{\infty} C_v^j \cdot (p_C)^j \cdot (1-p_C)^{v-j}. \quad (11)$$

In General, considering that the construction of each of the L chains – is an independent event, the probability that at least one of them will exceed to the length of the chain from legal blocks:

$$p_{FC} = 1 - \prod_{i=0}^{L-1} (1 - p_{V^{N-i}}) =$$

$$= 1 - \prod_{i=0}^{L-1} \left\{ 1 - \sum_{v=i+2}^{\infty} \frac{((i+1)\times K)^v \times e^{-((i+1)\times K)}}{v!} \left[\sum_{j=v}^{\infty} C_v^j \cdot (p_C)^j \cdot (1-p_C)^{v-j} \right] \right\}. \quad (12)$$

The dependence of the probability p_{FC} on the parameter L is shown in Figure (8).

DOI 10.15588/1607-3274-2020-1-18

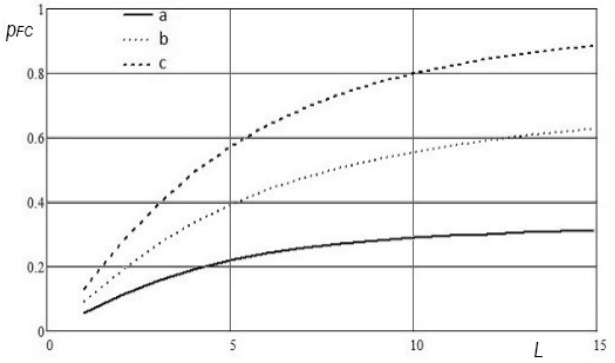


Figure 8 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, from the parameter L and the intensity of receiving extraneous blocks K for a fixed hash field length H =3
a) K = 3; b) K = 4; c) K =5

6 DISCUSSION

It can be seen that starting from L = 10, the increase of the probability of constructing a false chain is insignificant. The length of the hash field has the greatest impact on this probability. In the Figure (9) shows the dependence of p_{FC} on H and K. The region, that the most significant of the absolute values fall for the probability of constructing a false chain, it occurs in the range from H = 3 to H = 6. In the same range, the influence of the parameter value of L on the required probability is significantly reduced.

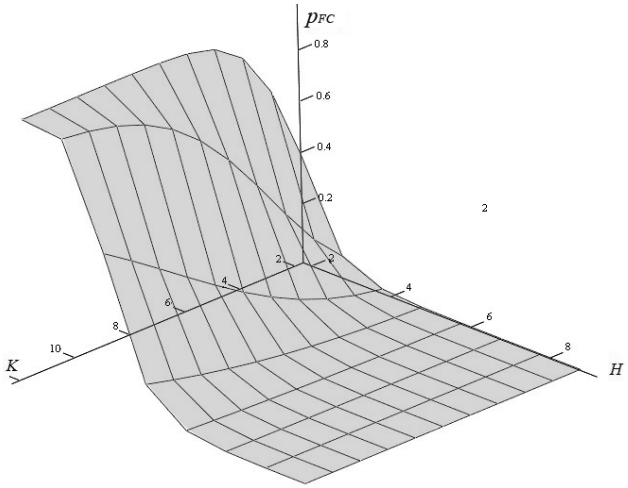


Figure 9 – graphs dependence on the probability of constructing a chain from extraneous blocks that length longer than the number of legal blocks, the length of the hash field H and the intensity of receiving extraneous blocks K with L = 4

Figure (10) shows the relative dependence of the value of p_{FC} on H for different values of L. For 1 at each point, the probability of constructing a false chain at L = 18 is adopted. It can be seen, when H> 6, the parameter of L practically does not affect the final probability of p_{FC}. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at H> 6 is about1 10^{-3}, which it's acceptable for real information transmission systems.

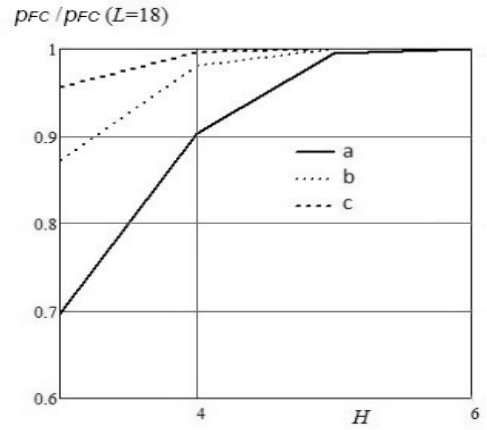


Figure 10 – Graph of the ratio of the value p_{FC} for different values of the parameter L to the value of p_{FC} at L = 18 (intensity of receiving extraneous blocks K = 5).
a) L = 6; b) L = 10; c) L =14

CONCLUSIONS

The above allows us to conclude that in the process of analyzing systems in which information is transmitted by block, when using the method of formation of information chains based on the method the hashes and the delivery time of the block, where we note, when the value of the hash field is equal to 6 or more, the probability of occurrence of duplicate branches is acceptably low. Where, when hash field more then 6, the parameter of length of a chain practically does not affect the final probability of constructing a chain from the extraneous blocks. The very same value of the probability of constructing a false chain, the length exceeding the chain of legal blocks at hash field more 6 is about1 10^{-3}, which it's acceptable for real information transmission systems.

ACKNOWLEDGEMENTS

This work was supported by the Federal State Budget Institution "Russian Foundation for Basic Research" on the basis of the grant "Research on the resistance of machine-based encryptors based on cellular automata to algebraic cryptanalysis" (Contract No. 19–31–90069 \ 19).

REFERENCES

1. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: NIST Special Publication 800–38A. Gaithersburg, Maryland, October 2010. 11p.
2. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800–38C. Gaithersburg, Maryland, May 2004. 25p.
3. Tanygin M. O., Tipikin A. P. Architecture of system of hardware restriction of access to information on a computer hard disk, *Telecommunications*, 2006, No. 3, pp. 44–46.
4. Knudson L. Block Chaining Modes of Operation. NIST First Modes of Operation Workshop [Electronic resource]. October 2010. Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.

DOI 10.15588/1607-3274-2020-1-18

5. Gervais A., Ghassan O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S. On the Security and Performance of Proof of Work Blockchains [Electronic resource], 2016. – Access mode: https://eprint.iacr.org/2016/555.pdf.
6. Black J., Rogaway P. and Shrimpton T. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Advances in Cryptology, *CRYPTO '00*. Santa Barbara, California, 2000, pp. 197–215.
7. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015, 152 p.
8. McGrew D., Viega J. The Security and Performance of the Galois/Counter Mode (GCM) of Operation, *In Proceedings: Indocrypt*, 2004, pp. 343–355.
9. Tanygin M.O. Method of Control of Data Transmitted Between Software and Hardware, *Computer Science and Engineering: Materials of the IV International Conference of Young Scientists CSE-2010*. Lviv, Publishing House of Polytechnics, 2010, pp. 344–345.
10. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code, *JCSS*, 1994, Vol. 3, No. 3, pp. 341–358.
11. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication, *Cryptologia*, 2010, pp. 225 – 23.
12. Stallings W. The Advanced Encryption Standard. Cryptologia, 2002, No. 26, pp. 165–188.
13. Tanygin M.O. Calculation of the probability of collisions when using the message authentication algorithm, *News SWSU*, 2012, pp. 179–183.
14. Gubarev A. V., Tanygin M. O. Research of dependence of time of searching legal instruction words from the width of the buffer the received instruction words, Telecommunications, 2015, pp. 21–26.
15. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality, *Cryptologia,* 34(2), pp. 163–175.
16. Tilborg H. C. Encyclopedia of Cryptography and Security. Heidelberg, Springer, 2005, pp. 11–15.
17. Lipmaa H. P., Rogaway P., and Wagner D. CTR Mode Encryption. NIST First Modes of Operation Workshop [Electronic resource]. Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
18. Voydock V., Kent S. Security Mechanisms in High-Level Network Protocols, *Computing Surveys,* June 1983, pp. 135–171.
19. Tanygin M.O., Search and elimination of collisions in information exchange through open communication channels, *Problems of Informatics in Education, Management, Economics and Technology: a collection of articles of the Xth International Scientific and Technical Conference.* Penza, Privolzhsky House of Knowledge, 2010. pp. 62–64.

Received 30.05.2019.
Accepted 23.11.2019.

УДК 004.056

МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ ПЕРЕДАНИХ БЛОКІВ ІНФОРМАЦІЇ

Танигін М. О. – канд. техн. наук, доцент, завідувач кафедрою інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

Алшаиа Х. Я. – аспірант кафедри інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

Кулешова О. О. – аспірант кафедри інформаційної безпеки, Південно-Західний державний університет, м. Курськ, Росія.

АНОТАЦІЯ

Актуальність. У статті приділено увагу всебічному вивченню проблем, що викликають передачу інформації у вигляді окремих блоків даних (кадрів, фреймів).

Метод. Описані методи контролю цілості у таких способах передачі. Детально розглянуто метод на основі ґешів і часу доставки блоку, проаналізованих методами зниження ймовірності помилок, відновлюючих прийомів при приєднанні окремих блоків інформації.

Результати. У процесі аналізу систем, в яких інформація передається блоком, при використанні методу формування інформаційних ланцюгів на основі методу хешів і часу доставки блоку, де ми зазначаємо, коли значення ґеш-поля дорівнює 6 і більше, ймовірність появи повторюваних гілок є прийнятно низькою. Де, коли ґеш-поле більше 6, параметр довжини ланцюга практично не впливає на остаточну ймовірність побудови ланцюга із сторонніх блоків. Саме це значення ймовірності побудови помилкового ланцюга, довжина якого перевищує ланцюжок легальних блоків у ґеш-полі більше 6 становить приблизно 10^{-3}, що є прийнятним для реальних систем передачі інформації.

Висновки. На основі проведеного аналізу можна зробити висновок, що в системах, в яких інформація передається поблоково, при використанні методу формування інформаційних ланцюжків на основі ґешу і часу надходження блоку, при величині поля ґешу від 6 і більше ймовірність виникнення дублюючих гілок є прийнятно низьклю.

КЛЮЧОВІ СЛОВА: розрахунок ймовірності, повідомлення обмеженої довжини; контроль автентичності; довжина ґеш-поля; дублювання гілок у ланцюжку.

УДК 004.056

МЕТОД КОНТРОЛЯ ЦЕЛОСТНОСТИ ПЕРЕДАВАЕМЫХ БЛОКОВ ИНФОРМАЦИИ

Таныгин М. О. – канд. техн. наук, доцент, заведующий кафедрой информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

Алшаиа Х. Я. – аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

Кулешова Е. А. – аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Россия.

DOI 10.15588/1607-3274-2020-1-18

АННОТАЦИЯ

Актуальность. В статье уделяется внимание всестороннему изучению проблем, возникающих при передаче информации в виде отдельных блоков данных (кадров, фреймов).

Метод. Описаны методы контроля целостности в таких способах передачи. Детально рассмотрен метод на основе хешей и времени доставки блока, проанализированы методы снижения вероятности ошибок, возникающих в приёмнике при приёме отдельных блоков информации.

Результаты. В процессе анализа систем, в которых информация передается по блокам, при использовании метода формирования информационных цепочек на основе метода хэшей и время доставки блока, где мы отмечаем, когда значение хеш-поля равно до 6 или более, вероятность появления дублирующих ветвей является приемлемо низкой. Когда хеш-поле больше 6, параметр длины цепочки практически не влияет на конечную вероятность построения цепочки из посторонних блоков. Само же значение вероятности построения ложной цепочки, длина которой превышает цепочку допустимых блоков в хэш-поле больше 6, составляет примерно 10^{-3}, что приемлемо для реальных систем передачи информации.

Выводы. На основе проведенного анализа можно сделать вывод, что в системах, в которых информация передаётся поблоково, при использовании метода формирования информационных цепочек на основе хеша и времени поступления блока, при величине поля хеша от 6 и более вероятность возникновения дублирующих ветвей приемлемо низка.

КЛЮЧЕВЫЕ СЛОВА: расчет вероятности, сообщения ограниченной длины, контроль подлинности, длина хеш-поля, дублирование ветвей в цепочке.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: NIST Special Publication 800–38A. Gaithersburg, Maryland, October 2010. 11p.
2. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800–38C. Gaithersburg, Maryland, May 2004. 25p.
3. Tanygin M. O. Architecture of system of hardware restriction of access to information on a computer hard disk / M. O. Tanygin, A. P. Tipikin // Telecommunications. – 2006. – № 3. – P. 44–46.
4. Knudson L. Block Chaining Modes of Operation. NIST First Modes of Operation Workshop [Electronic resource] / L. Knudson. – October 2010. – Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
5. Gervais A. On the Security and Performance of Proof of Work Blockchains [Electronic resource] / [A. Gervais, O. Ghassan, K. Wüst et al.] – 2016. – Access mode: https://eprint.iacr.org/2016/555.pdf.
6. Black J. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Advances in Cryptology / J. Black, P. Rogaway, and T. Shrimpton // CRYPTO ‘00. – Santa Barbara, California. – 2000. – P. 197–215.
7. Swan M. Blockchain: Blueprint for a New Economy / M. Swan. – O’Reilly Media, Inc., 2015. – 152 p.
8. McGrew D. The Security and Performance of the Galois/Counter Mode (GCM) of Operation / D. McGrew, J. Viega // In Proceedings: Indocrypt. – 2004. – P. 343–355.
9. Таныгин М. О. Метод контроля данных, передаваемых между программным и аппаратным обеспечением / М. О. Таныгин // Информатика и вычислительная техника: материалы IV Международной конференции молодых ученых CSE-2010. – Львов : Изд-во Политехники, 2010 – С. 344–345.
10. Bellare M. The security of the cipher block chaining message authentication code / M. Bellare, J. Kilian, P. Rogaway // JCSS. – 1994. – Vol. 3, No. 3. – P. 341–358.
11. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication / W. Stallings // Cryptologia. – 2010. – P. 225–23.
12. Stallings W. The Advanced Encryption Standard. Cryptologia. – 2002. – № 26. – P. 165–188.
13. Таныгин М.О. Расчет вероятности коллизий при использовании алгоритма аутентификации сообщений / М.О. Таныгин // Новости ЮУрГУ. – 2012. – С. 179–183.
14. Губарев А. В. Исследование зависимости времени поиска юридического слова инструкции от ширины буфера полученного слова инструкции / А. В. Губарев, М. О. Таныгин // Телекоммуникации. – 2015 – С. 21–26.
15. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality / W. Stallings // Cryptologia. – 34(2). – P. 163–175.
16. Tilborg H. C. Encyclopedia of Cryptography and Security / H. C. Tilborg // Heidelberg: Springer. – 2005. – P. 11–15.
17. Lipmaa H. CTR Mode Encryption. NIST First Modes of Operation Workshop [Electronic resource] / H. P. Lipmaa, P. Rogaway, and D. Wagner. – Access mode: http://csrc.nist.gov/groups/ST/toolkit/BCM/workshops.html.
18. Voydock V. Security Mechanisms in High-Level Network Protocols / V. Voydock, S. Kent // Computing Surveys. – June 1983. – P. 135–171.
19. Таныгин М. О. Поиск и устранение коллизий при обмене информацией по открытым каналам связи / М. О. Таныгин // Проблемы информатики в образовании, управлении, экономике и технологии: сборник статей X Международной научно-технической конференции. – Пенза : Приволжский Дом знаний. – 2010. – С. 62–64.

DOI 10.15588/1607-3274-2020-1-18

УПРАВЛІННЯ У ТЕХНІЧНИХ СИСТЕМАХ

CONTROL IN TECHNICAL SYSTEMS

УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

UDC 681.513

ALGORITHMS FOR TUNING OF THE COORDINATING AUTOMATIC CONTROL SYSTEMS

Gurskiy A. A. – PhD, Associate Professor of the Department of Technological Processes Automation and Robot-technical Systems, Odessa National Academy of Food Technologies, Odessa, Ukraine.

Goncharenko A. E. – PhD, Associate Professor, Associate Professor of the Department of Technological Processes Automation and Robot-technical Systems, Odessa National Academy of Food Technologies, Odessa, Ukraine.

Dubna S. M. – Lecturer of the Department of Technological Processes Automation and Robot-technical Systems, Odessa National Academy of Food Technologies, Odessa, Ukraine.

ABSTRACT

Context. The important task was solved during the scientific research related to the development of the algorithm for tuning of the coordinating automatic control system. The reason why the development of those algorithms is important is because of the progress in field of certain classes of complex multilayered control systems, which provide coordination of the transient processes while the regulating technological parameters.

Objective. The purpose of the scientific work is the minimizing of time and the automation of tuning process for the complex multilevel control systems.

Method. We offer the step-by-step tuning of the double-level coordinating systems of automatic control for the refrigeration facilities in the particular for the refrigerating turbocompressor facilities and systems with the tunnel refrigerating chambers. We offer the block-scheme of algorithms which may be used during the realization of automatic search for the system tuning parameters providing coordination of the transient processes under automatic control.

Results. The experiments were conducted in the Matlab 2012a environment. The result of the experiments is graphs of certain transient processes obtained on various steps of the tuning for multilevel coordinating automatic control system. Based on the simulation results we have done the conclusion about efficiency of the different algorithms. The possibility for using of the presented algorithms was also considered, particularly the specificity of the functioning of the automatic tuning of the automatic control multilevel system complex.

Conclusion. These experiments have showed the applicability of certain algorithms of step-by-step tuning for the double-level coordinating automatic control system. It is estimated, that the automatic tuning of the automatic control coordinating systems with algorithm utilization will increase the scope of the modern intellectual technologies.

KEYWORDS: Petri net, coordinating automatic control system, coordination of transient processes, ratio control, algorithms of tuning.

ABBREVIATIONS

CACS is a coordinating automatic control system;
ACS is an automatic control system.

NOMENCLATURE

$G_{x.a}$ is a compressor capacity;
π_k is a degree of pressure increase;
$\varphi(t)$ is a deviation from ratio of variables;
X_1 is an actual value of the controlled variable;
$P_{kip.z}$ is a set point of the boiling pressure;
P_{kip} is an actual value of the boiling pressure;
$e(t)$ is a deviation of the controlled variables within time;
J_{0i} is an integral criterion of system;
u_1, % is a control action on the flow of cooling water on the condenser;
u_2, % is a control action linked to the speed of rotation of the compressor shaft of the refrigeration plant;
u_a is a control action to change the ratio;
A^T is a coefficient matrix;
p is a differential operators.

DOI 10.15588/1607-3274-2020-1-19

INTRODUCTION

The coordination of transient is implemented in the range of multilevel automatic control systems. The lower level of such systems is linked to the liquidation of deviations from the ratio of the values of regulated variables. The upper level is linked to the liquidation of errors in the system. In the 20th century the well-known scientists Ignatienv M. B., Boichuk L. M. explored actively the systems under consideration [1–3]. Nowadays the coordinating control systems for refrigeration plants are designed. The development of these systems is carried out in the field of technological tasks [4, 5]. On this subject there are plenty of the similar scientific papers [6, 7], for example, in the field of control in the robotic systems [8–10] or in the field of air-fuel ratio control in the engines [11–13].

The design methods of coordinating automatic control systems were well represented in the scientific work by Boichuk L. M. [2]. In our days a lot of research centres explore the various automatic control systems and the corresponding methods of designing and analysis. These methods in designing of the systems of coordinating control are presented for the certain field of linear systems [3]. Therefore the design of tuning algorithms of control systems presented in scientific papers [4, 5, 10] is **relevant**. As these systems in the certain cases belong to the field of nonlinear systems. At the same time, these systems develop as the specific class of multilevel automatic control systems, thereby confirming the relevance of developing appropriate algorithms of tuning.

The object of study is the processes of tuning up of the coordinating automatic control systems.

The subject of study is the methods and algorithms of tunings for the coordinating automatic control systems.

The purpose of the scientific work is to minimize the time and automate of process in tuning of the multilevel coordinating automatic control systems.

1 PROBLEM STATEMENT

To achieve this purpose it is necessary to design the algorithms of tuning for the corresponding multilevel control systems. These algorithms of tuning are required to design for the complex non-linear control systems for which the known methods of synthesis are unacceptable.

As a result of analysis of the developed algorithms for tuning of the multilevel systems it is important for us to determine their fundamental suitability. It is also necessary to determine the scope of application for these algorithms in the system of automatic tuning with the intelligent technology. This intellectual system was shown in scientific work [14, 15] related to the automatic synthesis of Petri nets based on functioning of the neural networks.

The developed algorithms for tuning of the multilevel control system are acceptable, if they allow to determine all the values of the parameters $K \in k_{ij}$ of various levels for the control system. These parameters of tuning $K \in k_{ij}$ must give the minimum value of the integral criterion J in the multilevel system. The integral criterion of system is:

$$J = \int_0^\infty (|e(t)| + \beta \cdot |\phi(t)|)dt \to \min , \qquad (1)$$

where β is coefficient indicating the temporal coordination of the control processes; $\varphi(t)$ is deviations from the ratio of the values of regulated variables; $e(t)$ is the deviation of some variable in time from the given value.

2 REVIEW OF THE LITERATURE

Ratio systems controls or coordinating control systems have researched in the different countries. The design of these systems has not lost its relevance in the 21st century. Now there are a number of English scientific works related to the development the air-fuel ratio control systems for engines. In these works [11–13, 16] the control systems block diagrams are presented. They can also be classified as the multilevel coordinating automatic control systems.

In Ukraine there are a lot of scientific works [8–10] relayed to the control of robotic manipulators. The special cases of the implementation of the trajectory tasks of the coordinating control are presented in these scientific works. The scientific papers of Ignatiev M. B, Miroshnik I. V., Boychuk L. M., Tsybulkin G. A. [2, 3, 8, 17] are considered as the fundamental scientific works in the design of the corresponding systems.

The scientific work by Boychuk L. M. [2] has become the basis for the design of some control systems for refrigeration plants. First of all this is the design of the coordinating automatic control system model providing the energy-efficient functioning of the cooling turbocompressor plant [4]. Then the system was presented for evaluating of the energy efficiency of the functioning of a turbo-compressor plant for ammonia overload at the Odessa Port Plant [18]. The next stage was the development of control system for the laboratory unit with the cooling tunnel chamber [5]. Considering these scientific papers [4, 5, 10] it is possible to present the general simplified block diagram of the coordinating automatic control system. This block diagram is shown in figure 1. This control system represents the principles of operation and the main features of the architecture described in the scientific papers by Boichuk L. M. and Miroshnika I. V. [2]. However, such control system differs from similar systems presented in various papers [2, 8, 11, 19, 20].

There are the following main differences of the coordinating automatic control system under consideration from similar systems.

1. The control signals are formed as the sum of control signals of the lower and upper levels of the system.

2. There is an adjustment of the given ratio of parameters based on the automatic optimizer.

3. The control is implemented in the field of nonlinear systems.

4. There are no internal control loops at the lower level of the CACS.

Accordingly, we need methods for tuning of the coordinating automatic control system and in order to these

DOI 10.15588/1607-3274-2020-1-19

methods would be acceptable not only in the class of well-known linear systems [2, 3]. In this regard, this paper shows presents experiments related to the tuning of systems in this class.

3 MATERIALS AND METHODS

The considered coordinating automatic control system is two-level. The lower (first) level of control in this system is linked to the liquidation of deviation from the ratio of the values of regulated variables X_1 and X_2. And the upper (second) level of control is linked to the liquidation of the difference between the set and the actual value of the controlled variable.

This coordinating control system adjusts to the deviding of motions mode. It lets to eliminate the deviation from the ratio of variables X_1 and X_2 in the transition process is linked to the liquidation of error in the system. This is shown graphically in Fig. 1. The movement of the system from the initial point X_0 to the final X_k in the space of variables X_1 and X_2 is shown. Movement along the trajectory 1 corresponds to the traditional automatic control system and movement along the trajectory 2 corresponds to the coordinating automatic control system. The deviding of motions mode provides the initial motion towards the multitude M of the ratios, and then by the multitude M to the end point X_k.

In the MATLAB \ Simulink software environment we have implemented the model of coordinating automatic control system for the development of the tuning algorithms (Fig. 2). The refrigeration turbocompressor is the control object in this system. The refrigeration turbocompressor model is represented as the linear system. It gives some error in the simulation results. However this inaccuracy does not interfere with scientific research for the design of methods for the synthesis of CACS.

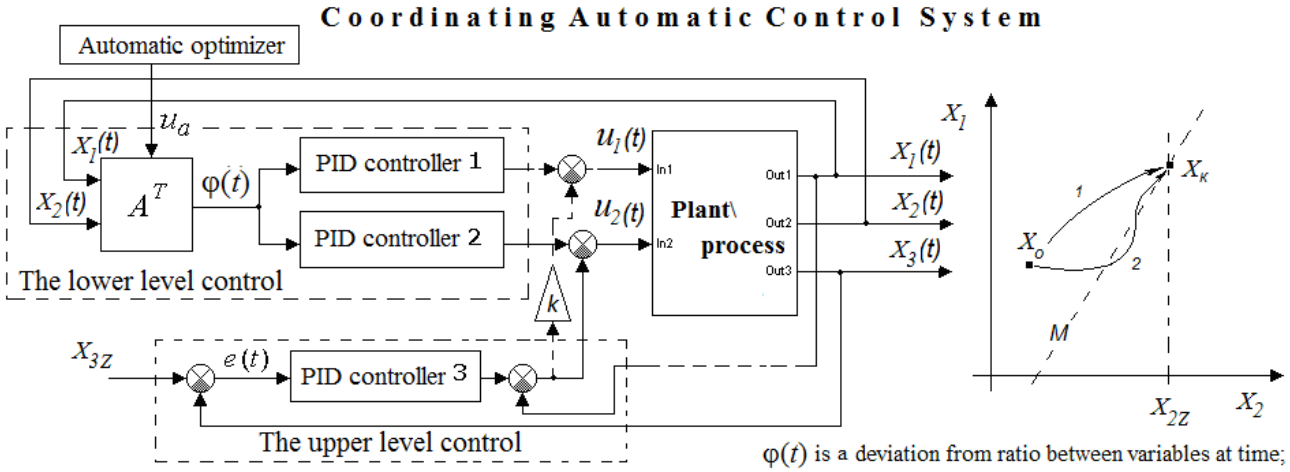


Figure 1 – The simplified block diagram of the coordinating automatic control system

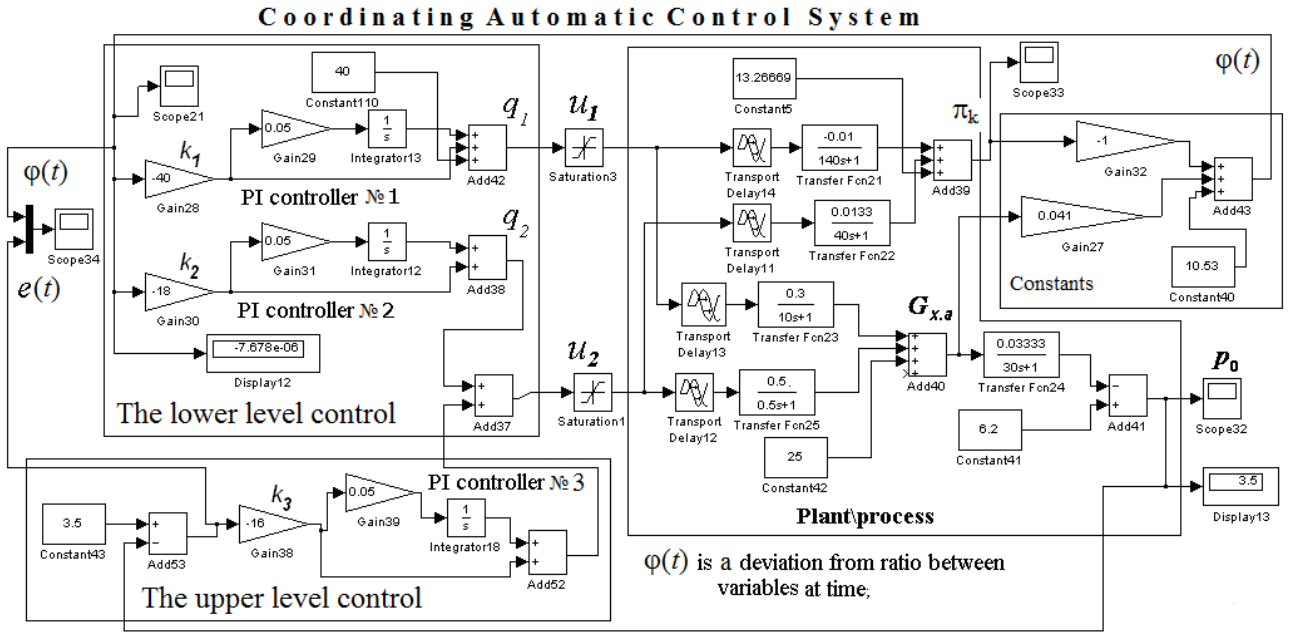


Figure 2 – Block diagram of the model of the coordinating automatic control system presented by means of the MATLAB \ Simulink software environment

DOI 10.15588/1607-3274-2020-1-19

We have represented the system control law in the following way:

$$\overline{u} = \overline{u}_q + \overline{u}_p = \begin{bmatrix} u_1 & u_2 \end{bmatrix}^T , \quad (2)$$

where

$\overline{u}_q = \begin{bmatrix} u_{q1} \\ u_{q2} \end{bmatrix} = \begin{bmatrix} k_1 \cdot (1 + k_{11} \cdot p) \\ k_2 \cdot (1 + k_{21} \cdot p) \end{bmatrix} \cdot \phi$ is the law of lower level control;

$\overline{u}_p = \begin{bmatrix} u_{p1} \\ u_{p2} \end{bmatrix} = \begin{bmatrix} 0 \\ (P_{kip.z} - P_{kip}) \cdot k_3 (1 + k_{31} \cdot p) \end{bmatrix}$ is the law of upper level control;

$\phi = k \cdot G_{x.a} - \pi_k + b$ is the deviation from ratio of the parameters. This ratio ensures the functioning of the turbocharger with maximum efficiency; $\pi_k = p_k / p_0$ is degree of pressure increase; P_{kip} is actual value of the controlled variable; $P_{kip.z}$ is set point of the boiling pressure; $G_{x.a}$ is compressor capacity; p is differential operators; u_1, % is control action on the flow of cooling water on the condenser; u_2, % is control action linked to the speed of rotation of the compressor shaft of the refrigeration plant; k is coefficient for the ratio; b is constants.

The tuning of this system must be implemented taking into account for ensuring the necessary peculiarities of its functioning, Such as the coordinating change of compressor capacity $G_{x.a}$ and the degree of pressure increase $\pi_k = p_k / p_0$ during the regulation of the boiling pressure $P_{kip} \approx P_0$. The coordinating change of compressor capacity $G_{x.a}$ is possible within tuning of the system for deviding of motions mode.

The researches have shown that it is possible to define two main algorithms for the step-by-step tuning of the coordinating system to the deviding of motions mode.

At the beginning of the tuning all parameters k_1, k_2 and k_3 of the regulators №1, №2 and №3 are equal to zero.

According to the first algorithm the main regulator №1 of the 1st lower coordinating control level is set up initially. The tuning is implemented according to such integral criterion:

$$J_{01} = \int_0^\infty \phi^2(t) dt \to \min . \quad (3)$$

The transient characteristics for deviations from the ratio of variables at different values of the parameter k_1 of the regulator №1 and at corresponding values of the criterion J_{01} are presented in Fig. 3.

At the second stage the regulator №3 of the upper level of control is set up according to the integral criterion:

$$J_{02} = \int_0^\infty (|e(t)| + 3 \cdot |\phi(t)|) dt \to \min . \quad (4)$$

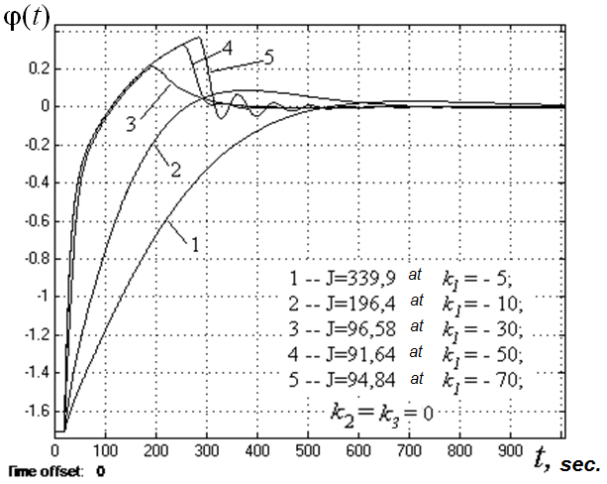


Figure 3 – The transient responses showing by deviation $\varphi(t)$ from the given ratio of variables within time. The transitional responses got at different values of the tunings parameters in the coordinating automatic control system

At the final stage regulator №2 of the 1st lower coordinating level of control is set up according to the criterion:

$$J_{03} = \int_0^\infty (|\phi(t)| + |e(t)|) dt \to \min . \quad (5)$$

All transient processes obtained at various stages of the system tuning setup are shown in Fig. 3–5.

The second algorithm of tuning consists of four stages. At the first stage the tuning of regulator of upper level according to the integral criterion is presented:

$$J_{00} = \int_0^\infty |e(t)| dt \to \min . \quad (6)$$

Then the regulator of coordinating level is set up according to the corresponding criterion:

$$J_{01} = \int_0^\infty |\phi(t)| dt \to \min . \quad (7)$$

At the third stage the tuning of upper level regulator №1 are adjusted again according to the criterion:

$$J_{02} = \int_0^\infty (2 \cdot |\phi(t)| + |e(t)|) dt \to \min . \quad (8)$$

At the last stage the regulator №2 of the coordinating level is adjusted according to the criterion:

$$J_{03} = \int_0^\infty (|\phi(t)| + |e(t)|) dt \to \min . \quad (9)$$

4 EXPERIMENTS

All necessary experiments were performed in the MATLAB \ Simulink 2012 software environment. Initially it is necessary to implement a model of the coordinating automatic control system to conduct experiments

DOI 10.15588/1607-3274-2020-1-19

in the software environment. The block diagram of this model is presented in Fig. 2. All parameters in the model of the control object and in the corresponding control system are also presented in Fig. 2. Possessing the appropriate software you can realize experiments using the necessary data presented only in Fig. 2–4. To verify the principle suitability of the considered algorithms we have obtained transients at various stages of the tuning in the control system. These transients and the corresponding parameters k_1, k_2, k_3 of the coordinating control system are presented in Fig. 4 and 5.

It is interesting to note the specific experiment shown in Fig. 6. If the control action of the upper level of the coordinating control system is connected with the control action u_1, then we must change accordingly the tuning of algorithms.

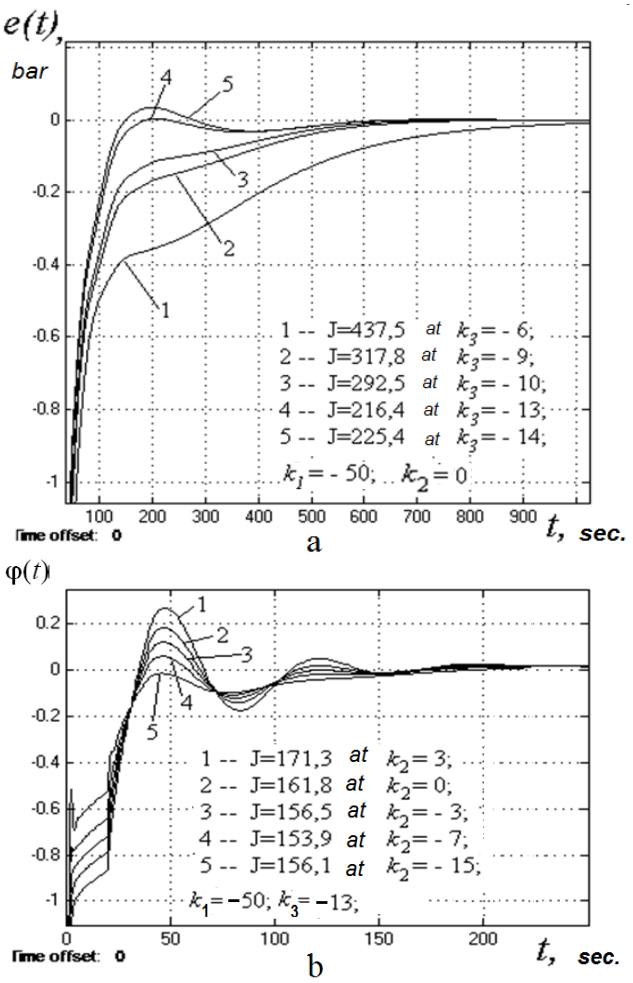


Figure 4 –The transient characteristics of the coordinating automatic control system at different values of the tunings. The transient characteristics showing the deviation $e(t)$ from the set value are presented in Fig. 4a. The transient characteristics showing the deviation $\varphi(t)$ from the given ratio of variables are presented in Fig. 4b.

The block diagram of such system is also shown in Fig. 6. As a result of modeling of this system it is possible to obtain the necessary transients. These transients processes fairly accurately represent the coordination of the regulatory processes and the tuning of the system to the deviding of motions mode.

We can see from the transient graphs that the deviation $\varphi(t)$ from the ratio of the variables was practically reduced to zero three times faster than the deviation $e(t)$ of the controlled variable from the set value (Fig. 6). According to the deviding of motions mode in the time interval from 200 seconds to 1200 seconds the movement was provided in the multitude of controlled ratio.

5 RESULTS

We can see from the graphs of transient processes presented in Fig. 3–5, the phased tuning of the coordinating automatic control system is carried out under the condition of its stable operation. The minimum value of the corresponding integral criterion and the corresponding values of the regulators tunings are determined at each stage of the control system tuning.

We can conclude based on the analysis of the simulation results obtained at various algorithms of the phased tuning of the coordinating control system. The four-step tuning algorithm provides slightly faster way for the system to reach the target multitude of controllable ratios (figures 5d and 4c). Accordingly, the value of the integral criterion of the quality (J_{03}=139.8) for the system is less with the four-stage algorithm than with the three-stage (J_{03} = 153.9).

6 DISCUSSION

The described tuning algorithms are phased due to the structural features of multi-level systems. This case is suitable not only for multi-level systems of the coordinated regulation. The tuning of cascade control system also presumes the phased tuning. For example, at first it is necessary to set the inside control loop and then to set the outer loop.

We should also note the scientific paper [2]. In this scientific paper there is some process of step-by-step system synthesis in which initially the coordinating control system is considered as the one-level control system and then as the multi-level one.

The phased tuning algorithms are represented in the form of flowcharts shown in Fig. 7 and accordingly, in the form of Petri nets in Fig. 8.

Petri net formation is the important component for representation of the tuning process of the control system. If the automatic tuning of the coordinating control system is carried out, then the formed Petri net represents to the user the definite process of retraining the specific artificial neural network. In this case the neural network represents the intellectual feature of the automatic tuning systems, i.e. such network is able to learn at the operation of various systems.

The simplified block diagram of control system with the automatic tuning algorithm is shown in Fig. 9. Thus, it is possible to set up the system to deviding of motions mode.

DOI 10.15588/1607-3274-2020-1-19

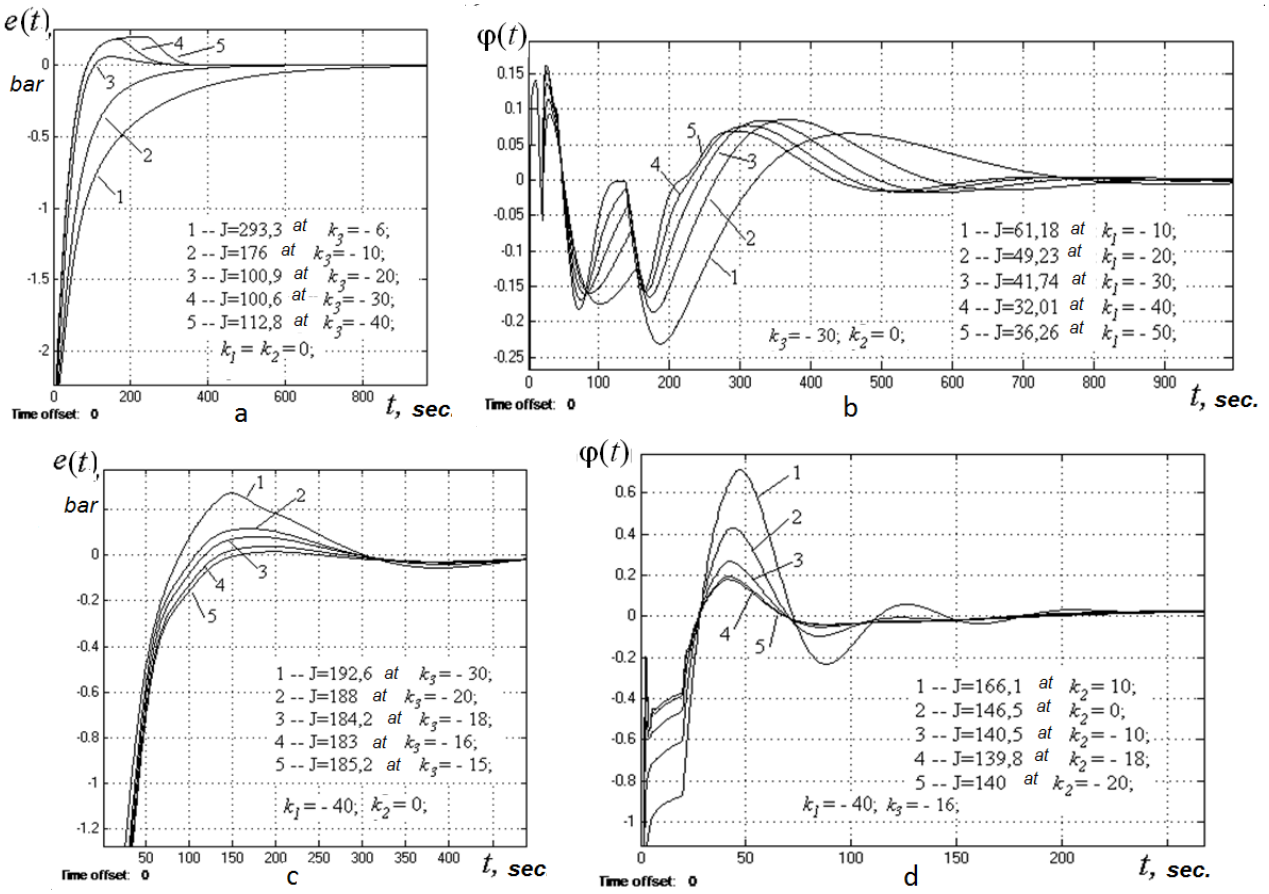


Figure 5 – Transients in the CACS for the different values in the parameters of the regulators. These transients are obtained at the stage of tuning by the four-step algorithm. Figure 4a and 4c – transient characteristics of the deviation $e(t)$ of the controlled variable from the specified value; figures 5b and 5d – transient characteristics of the deviation $\varphi(t)$ from the ratio of variables

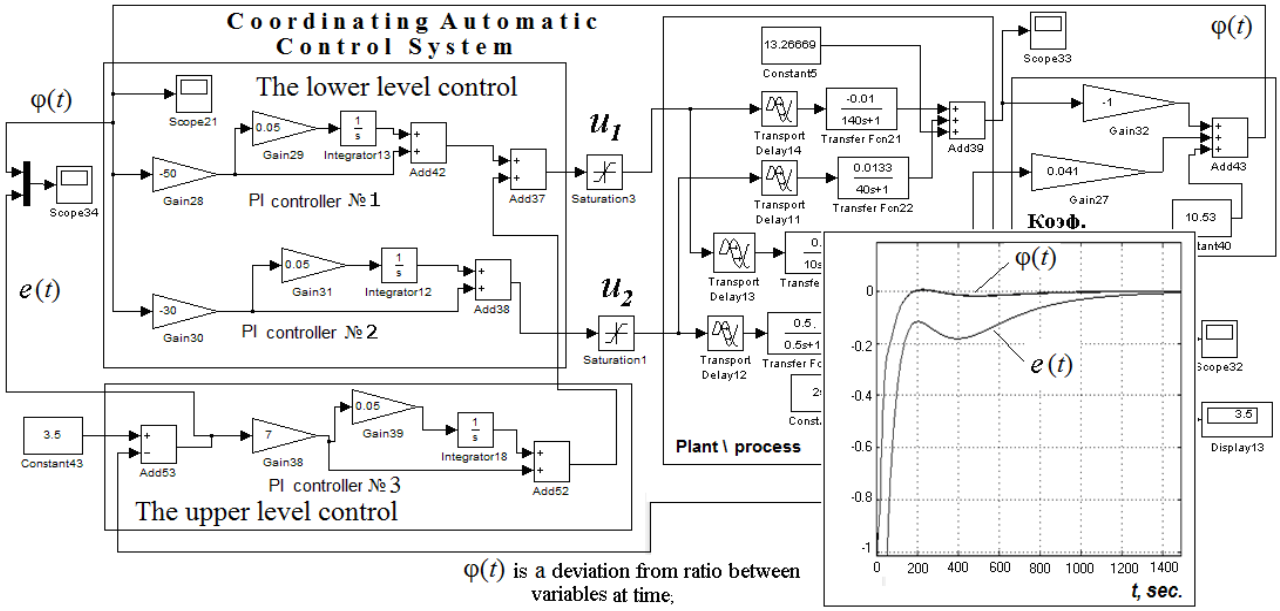


Figure 6 – Block diagram of the model of the coordinating control system and the graphs of transient processes on the deviation $\varphi(t)$ from the ratio of the values of the controlled variables and on the deviation $e(t)$ of the regulable variable from the specified value

The artificial neural network forms the algorithm for tuning the control system in the kind of Petri net, it is just shown in Fig. 9. If the algorithm of tuning for the control system is unsatisfactory, then the artificial neural network is rebuilt according to the formed Petri net. This algorithm for retraining of the artificial neural network was pre-

DOI 10.15588/1607-3274-2020-1-19

sented in the scientific work [15] as the first experience to implement this system.

CONCLUSIONS

The scientific novelty of the results. The problem associated with the development of tuning algorithms for the highlighted class of automatic control systems was solved in the present work. Thus the design technique of corresponding coordinating systems has got the further development.

The practical significance of the results. The completed scientific researchers have confirmed the suitability of the developed algorithms for tuning of the coordinating automatic control systems. Due to these algorithms we can solve the problem of automated tuning for models of the complicated control systems providing the coordination of various transients.

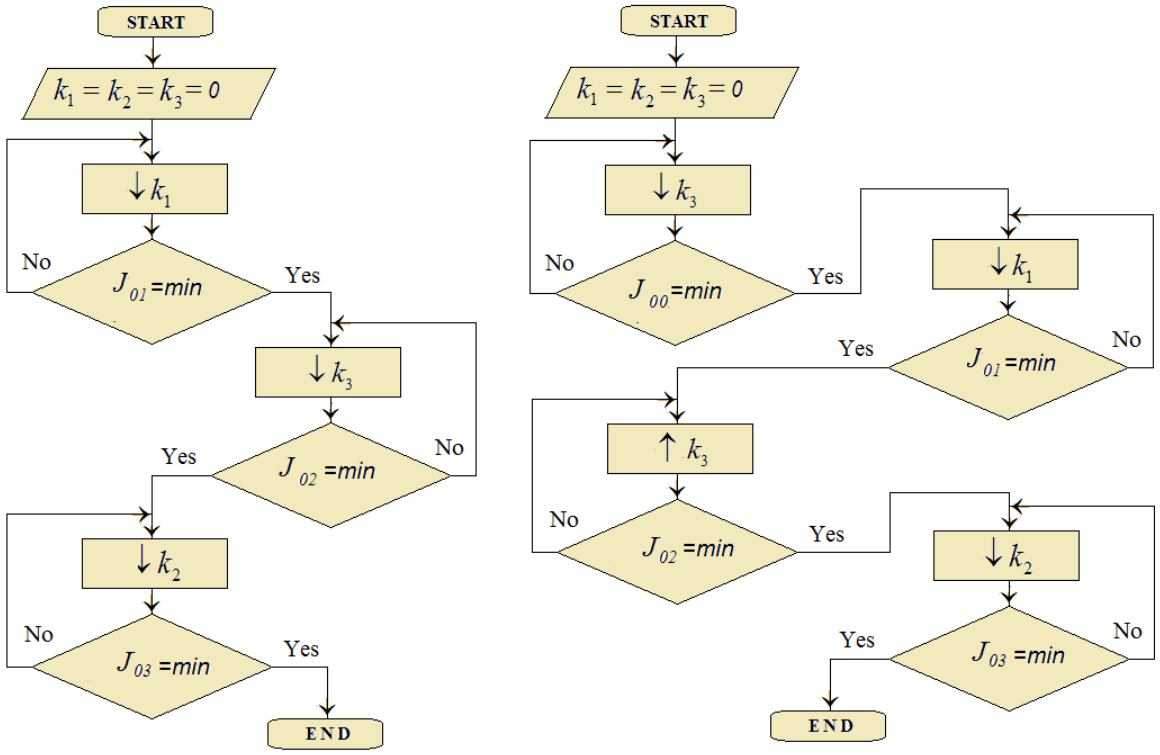
The prospects for further research. The problem of automated tuning for the coordinating control systems may be related to the field of automatic generation of Petri nets and to the field the learning of neural nets, namely, the self-learning of neural networks at the synthesis of Petri nets.

ACKNOWLEDGMENTS

The scientific work was carried out at the department of technological processes automation and robotic systems.

The authors would like to give thanks N. Pantelyuk. He heads the laboratory for automation of refrigeration machines and plant. He designed the laboratory plant with a tunnel cooler. The corresponding studies of various control algorithms were carried out at this laboratory plant.

The authors also would like to give thanks the leadership of the Odessa Refinery Plant. The Odessa Refinery Plant has given experimental data related to ammonia cooling. These experimental data were necessary to complete a number of scientific works in the sphere of modeling automatic coordinating control systems.



$$J_{01} = \int_0^\infty \varphi^2(t)\,dt \to \min = 91{,}64 \quad at \quad k_1 = -50;$$

$$J_{02} = \int_0^\infty (|e(t)| + 3\cdot|\varphi(t)|)dt \to \min = 216{,}4 \quad at \quad k_3 = -13;$$

$$J_{03} = \int_0^\infty (|\varphi(t)| + |e(t)|)dt \to \min = 153{,}9 \quad at \quad k_2 = -7;$$

$$J_{00} = \int_0^\infty |e(t)|dt \to \min = 100{,}6 \quad at \quad k_3 = -30;$$

$$J_{01} = \int_0^\infty |\varphi(t)|dt \to \min = 32{,}01 \quad at \quad k_1 = -40;$$

$$J_{02} = \int_0^\infty (2\cdot|\varphi(t)| + |e(t)|)dt \to \min = 183 \quad at \quad k_3 = -16;$$

$$J_{03} = \int_0^\infty (|\varphi(t)| + |e(t)|)dt \to \min = 139{,}8 \quad at \quad k_2 = -18;$$

Figure 7 – Flowcharts representing the phased tuning of the coordinating automatic control system; ↓ $k1$, ↓ $k2$ and ↓ $k3$ are decrease in the values of the parameters $k1$, $k2$ and $k3$; ↑ $k3$ is increase in the value of the $k3$ parameter

DOI 10.15588/1607-3274-2020-1-19

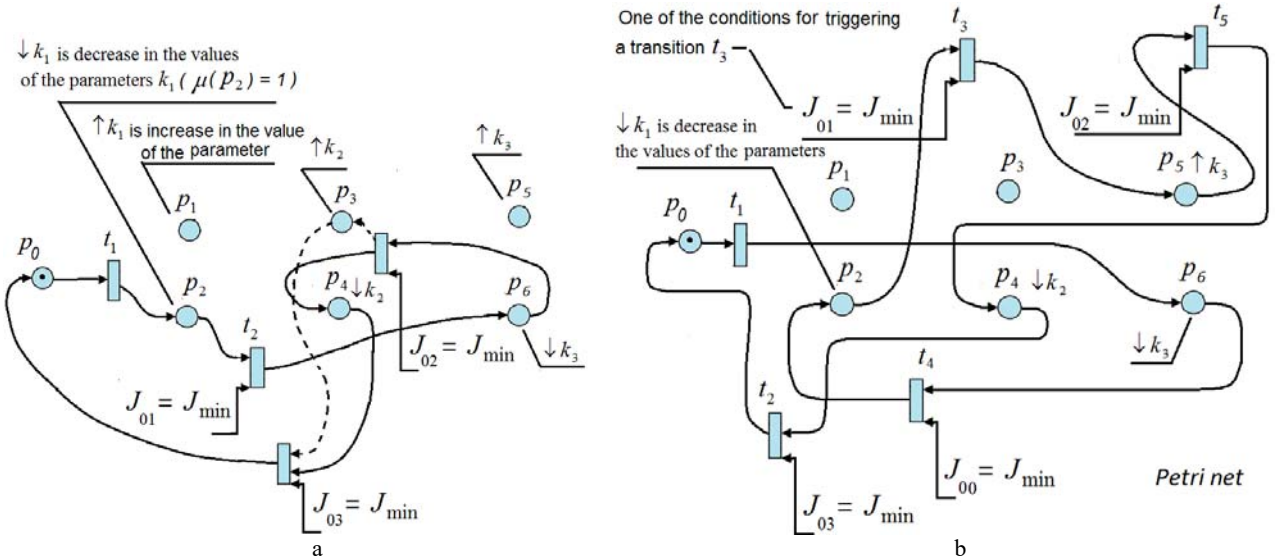


Figure 8 – The Petri nets representing the algorithms of phased tuning for the CACS. The Petri net representing the three-step algorithm for tuning of the coordinating automatic control system is shown at Fig. 8a. The Petri net representing the corresponding four-step algorithm of tuning is shown at Fig. 8b.

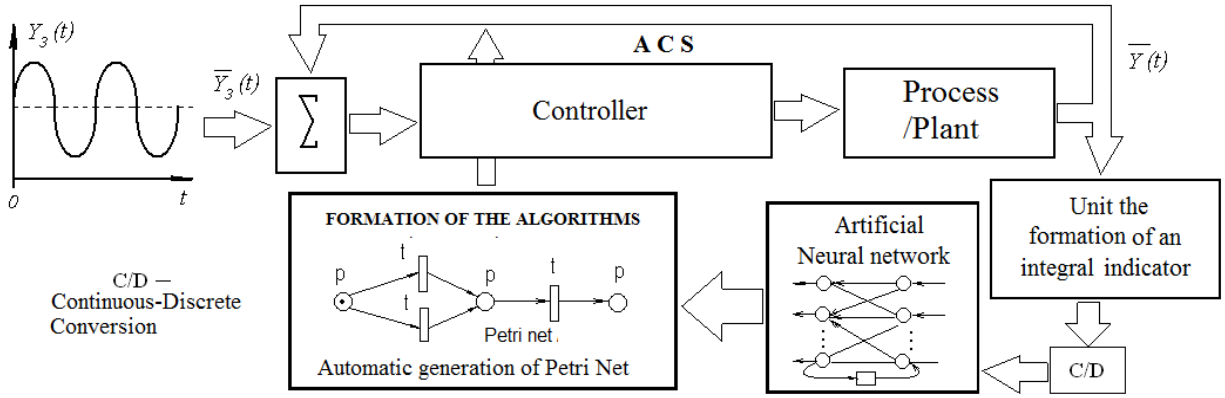


Figure 9 – The simplified block diagram of the control system with algorithm of the automatic tuning

REFERENCES

1. Boichuk L. M., Kratov G. I., Dykhanov V. P. Controlling a Long String of Moving Vehicles via Dynamic Coordination Technique, *IFAC Proceedings Volumes*, 1995, Vol. 28, No. 10, pp. 165–168. DOI: https://doi.org/10.1016/S1474-6670(17)51511-6
2. Boichuk, L. M. Synthesis of coordinated systems of automatic control. Moscow, Energoatomizdat, 1991, 160 p. ISBN 5–283–01521–1
3. Filimonov A. B., Filimonov N. B. The issues of synthesis for coordinating automatic control systems, *Izvestiya SfedU, Engineering sciences*, 2012, Vol. 3, pp. 172–180. ISSN 1999–9429 2311–3103
4. Gurskiy A., Denisenko V., Goncharenko A. Systems of refrigerating centrifugal compressors capacity automatic control, *Refrigeration Engineering and Technology*, 2013, No. 5, pp. 72–76. ISSN 0453-8307
5. Dubna S. M., Gurskiy A. A., Goncharenko A. E. The working out of algorithms in control of the cooling processes of products in the tunnel cameras, *Refrigeration Engineering and Technology*, 2018, No. 5, pp. 72–76. ISSN 0453-8307
6. Romanenko V. D., Milyavsky Yu. L. The design of coordinating control algo-rithm for the thermal mixing aggre-gate under external dis-turbances, Research Bulletin of NTUU "Kyiv Polytechnic Institute", 2011, No. 1, pp. 84–89. ISSN 1810-0546
7. Romanenko V. D., Milyavsky Yu. L. Multivariate object coordinating control with multirate sampling in stochastic environment, *System research & information technologies*, 2011, No 2, pp. 7–20. ISSN 2308-8893 (Online).
8. Tsybulkin G. A. Two-level coordinating control of a manipulation robot with kinematic redundancy, *Problems of Control and Informatics*, 1995, No. 3, pp. 143–150. ISSN 0572-2691
9. Tsybulkin G. A. The corrective automatic control of trajectory. Kiev, Stal, 2012, 161 p. ISBN 978–617–676–011–5
10. Gurskiy A. A., Goncharenko A. E., Dubna S. M. Coordinating automatic control systems of the robot manipulator drivers, *Automation of technological and business processes,* 2018, No. 4, pp. 11–21. ISBN 2312–3125
11. Chatlatanagulchai W., Rhienprayoon S., Yaovaja K., Wannatong K. Air/fuel ratio control in diesel-dual-fuel engine by varying throttle, *EGR valve, and total fuel. – SAE Technical Paper*, 2010, Issue 2010-01-2200. DOI: https://doi.org/10.4271/2010-01-2200
12. Jiao X., Zhang J., Shen T., Kako J. Adaptive air-fuel ratio control scheme and its experimental validations for port-injected spark ignition engines, *International Journal of Adaptive Control and Signal processing*, 2015, Volume 29, Issue 1, pp. 41–63. DOI: 10.1002/acs.2456.
13. Wong H., Wong P., Vong C. Model predictive engine air-ratio control using online sequential relevance vector machine, *Journal of Control Science and Engineering*, 2012, Vol. 2012, P. 2. DOI:10.1155/2012/731825.
14. He D. W., Strege B., Tolle H., Kusiak A. Decomposition in automatic generation of Petri nets for manufacturing system control and scheduling, *International Journal of Production Re-*

DOI 10.15588/1607-3274-2020-1-19

search, 2000, Vol. 38, Issue 6, pp. 1437–1457. DOI: 10.1080/002075400188942
15. Gurskiy A. A., Dubna S. M. Tuning of neural network during automatic synthesis of Petri nets, *Automation of technological and business processes,* 2018, No. 1, pp. 22–32. DOI: https://doi.org/10.15673/ atbp.v10i1.877
16. ZENG Ting-jian, LUO Zhi-hao, CHEN Bo, LI Shu-wei, YIN Feng Analysis and Optimization of Coordination Control System for Ultra Supercritical Power Generation Unit, *DEStech Transactions on Environment, Energy and Earth Sciences 2017 (ICEPEE 2017)*, 2017, pp. 349–352. DOI 10.12783/dteees/icepe2017/11864
17. Miroshnik, I.V. Consistent control by multi-channel systems. Leningrad, Energoatomizdat, 1990, 128 p. ISBN 5-283-04476-9.
18. Gurskiy A. A., Denisenko A.V., Goncharenko A. E. Deficiency on the ratio parameters in a control system as a parameter of turbo compressor plant functioning, *Refrigeration Engineering and Technology,* 2014, No. 4, pp. 58–64. ISSN 0453-8307
19. Markus Elisha D., Yskander Hamam, Agee John T., Adisa Jimoh A. Coordination control of robot manipulators using flat outputs, *Robotics and Autonomous Systems,* 2016, Vol. 83, pp 169–176. https://doi.org/10.1016/ j.robot.2016.05.006
20. Gan Yahui, Duan Jinjun, Chen Ming, Dai Xianzhong Multi-Robot Trajectory Planning and Posi-tion/Force Coordination Control in Complex Welding Tasks, *Applied Sciences,* 2019. 9(5), 924, P. 23. https://doi.org/10.3390/ app9050924

Received 09.01.2020.
Accepted 20.02.2020.

УДК 681.513

АЛГОРИТМИ НАСТРОЮВАННЯ КООРДИНУВАЛЬНИХ СИСТЕМ АВТОМАТИЧНОГО УПРАВЛІННЯ

Гурський О. О. – канд. техн. наук, доцент кафедри автоматизації технологічних процесів і робототехнічних систем інституту комп'ютерних систем і технологій «Індустрія 4.0» ім. П. Н. Платонова Одеської національної академії харчових технологій, Одеса, Україна.

Гончаренко О. Є. – канд. техн. наук, доцент кафедри автоматизації технологічних процесів і робототехнічних систем інституту комп'ютерних систем і технологій «Індустрія 4.0» ім. П. Н. Платонова Одеської національної академії харчових технологій, Одеса, Україна.

Дубна С. М. – старший викладач кафедри автоматизації технологічних процесів і робототехнічних систем інституту комп'ютерних систем і технологій «Індустрія 4.0» ім. П. Н. Платонова Одеської національної академії харчових технологій, Одеса, Україна.

АНОТАЦІЯ

Актуальність. Вирішена актуальна задача, що пов'язана з розробкою алгоритмів настроювання координувальних систем автоматичного управління. Важливість розробки даних алгоритмів викликана розвитком, у цей час, певного класу складних багаторівневих систем управління, що забезпечують узгодження перехідних процесів при регулюванні технологічних параметрів.

Мета роботи – мінімізація часу та автоматизація процесу настроювання багаторівневих координувальних систем автоматичного управління.

Метод. Запропоновано поетапне настроювання дворівневих координувальних систем автоматичного управління для об'єктів холодильної техніки, в окремому випадку для холодильних турбокомпресорних установок і систем з тунельними холодильними камерами. Наводяться блок-схеми алгоритмів, які можуть бути використані на етапі автоматизованого пошуку параметрів настроювання системи, що забезпечує узгодження перехідних процесів при автоматичному управлінні.

Результати. Експерименти були проведені в середовищі Matlab 2012a, за результатами яких були отримані графіки певних перехідних процесів на різних етапах настроювання багаторівневої системи автоматичного управління. На підставі аналізу результатів моделювання робиться висновок про доцільність використання різних алгоритмів настроювання.

Також була визначена галузь застосування розроблених алгоритмів поетапного настроювання багаторівневих систем. В окремому випадку були представлені особливості функціонування комплексу автоматизованого настроювання багаторівневих систем автоматичного управління.

Висновки. Проведені експерименти показали принципову придатність певних алгоритмів поетапного настроювання дворівневих координувальних систем автоматичного управління. Встановлено, що реалізація автоматизованого настроювання координувальних систем автоматичного управління із застосуванням відповідних алгоритмів має місце в галузі сучасних інтелектуальних технологій.

КЛЮЧОВІ СЛОВА: координація, узгодження процесів, регулювання співвідношення, алгоритми настроювання, мережі Петрі.

УДК 681.513

АЛГОРИТМЫ НАСТРОЙКИ КООРДИНИРУЮЩИХ СИСТЕМ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

Гурский А. А. – канд. техн. наук, доцент кафедры автоматизации технологических процессов и робототехнических систем института компьютерных систем и технологий «Индустрия 4.0» им. П. Н. Платонова Одесской национальной академии пищевых технологий, Одесса, Украина.

Гончаренко А. Е. – канд. техн. наук, доцент кафедры автоматизации технологических процессов и робототехнических систем института компьютерных систем и технологий «Индустрия 4.0» им. П. Н. Платонова Одесской национальной академии пищевых технологий, Одесса, Украина.

Дубна С. М. – старший преподаватель кафедры автоматизации технологических процессов и робототехнических систем института компьютерных систем и технологий «Индустрия 4.0» им. П. Н. Платонова Одесской национальной академии пищевых технологий, Одесса, Украина.

АННОТАЦИЯ

Актуальность. Решена актуальная задача, связанная с разработкой алгоритмов настройки координирующих систем автоматического управления. Важность разработки данных алгоритмов вызвана развитием, в настоящее время, определенного класса сложных многоуровневых систем управления, обеспечивающих согласование переходных процессов при регулировании технологических параметров.

Цель работы – минимизация времени и автоматизация процесса настройки многоуровневых координирующих систем автоматического управления.

Метод. Предложена поэтапная настройка двухуровневых координирующих систем автоматического управления для объектов холодильной техники. В частном случае для холодильных турбокомпрессорных установок и систем с туннельными холодильными

DOI 10.15588/1607-3274-2020-1-19

камерами. Представляются блок-схемы алгоритмов, которые могут быть использованы на этапе автоматизированного поиска параметров настройки системы, обеспечивающей согласование переходных процессов при автоматическом управлении.

Результаты. Эксперименты были проведены в среде Matlab 2012a, в результате которых были получены графики определенных переходных процессов на различных этапах настройки многоуровневой системы автоматического управления. На основе анализа результатов моделирования делается вывод о целесообразности использования различных алгоритмов настройки.

Также была определена область применения разработанных алгоритмов поэтапной настройки многоуровневых систем. В частном случае были представлены особенности функционирования комплекса автоматизированной настройки многоуровневых систем автоматического управления.

Выводы. Проведенные эксперименты показали принципиальную пригодность определенных алгоритмов поэтапной настройки двухуровневых координирующих систем автоматического управления. Установлено, что реализация автоматизированной настройки координирующих систем автоматического управления с применением соответствующих алгоритмов имеет место в области современных интеллектуальных технологий.

КЛЮЧЕВЫЕ СЛОВА: координация, согласование процессов, регулирование соотношения, алгоритмы настройки, сети Петри.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Boichuk L. M. Controlling a Long String of Moving Vehicles via Dynamic Coordination Technique / L. M. Boichuk, G. I. Kratov, V. P. Dykhanov // IFAC Proceedings Volumes. – 1995. – T. 28, № 10. – P. 165–168. DOI: https://doi.org/10.1016/S1474-6670(17)51511-6
2. Boichuk, L. M. Synthesis of coordinated systems of automatic control [Sintez koordinirujushhih sistem avtomaticheskogo upravlenija] / L. M. Boichuk – Moscow, Energoatomizdat, 1991. – 160 p. ISBN 5–283– 01521–1
3. Filimonov A. B. The issues of synthesis for coordinating automatic control systems [O problematike sinteza koordiniruyuschih sistem avtomaticheskogo upravleniya] / A. B. Filimonov, N. B. Filimonov // Izvestiya SfedU, Engineering sciences. – 2012. – Vol. 3. – P. 172–180. ISSN 1999–9429 2311–3103
4. Gurskiy A. Systems of refrigerating centrifugal compressors capacity automatic control [Sıstemy avtomatıcheskogo regýlırovanııa proızvodıtelnostı holodılnyh tsentrobejnyh kompressorov] / A. Gurskiy, V. Denisenko, A. Goncharenko // Refrigeration Engineering and Technology. – 2013. – No. 5. – P. 72–76. ISSN 0453-8307
5. Dubna S. M. The working out of algorithms in control of the cooling processes of products in the tunnel cameras [Razrabotka algorıtmov ýpravlenıia protsessamı ohlajdenıia prodýktov v týnnelnyh kamerah] / S. M. Dubna, A. A. Gurskiy, A. E. Goncharenko, // Refrigeration Engineering and Technology. – 2018. – No. 5. – P. 72–76. ISSN 0453-8307
6. Romanenko V. D. The design of coordinating control algorithm for the thermal mixing aggregate under external disturbances [Razrabotka sistemi koordiniruyuschego cifrovogo upravleniya termosmesitelnoi ustanovkoi pri deistvii vneshnego vozmuscheniya] / V. D. Romanenko, Yu. L. Milyavsky // Research Bulletin of NTUU “Kyiv Polytechnic Institute”. – 2011. – No. 1. – P. 84–89. ISSN 1810-0546
7. Romanenko V. D. Multivariate object coordinating control with multirate sampling in stochastic environment [Koordinuyuche keruvannya bagatovimirnim ob’єktom iz riznotempovoyu diskretizacієyu v stohastichnomu seredovischi] / V. D. Romanenko, Yu. L. Milyavsky // System research & information technologies. – 2011. – No 2. – P. 7–20. ISSN 2308-8893
8. Tsybulkin G. A. Two-level coordinating control of a manipulation robot with kinematic redundancy [Dvýhýrovnevoe koordınırýıýee ýpravlenıe manıpýlıatsıonnym robotom s kınematıcheskoı ızbytochnostıý] / G. A. Tsybulkin // Problems of Control and Informatics. – 1995. – No. 3. – P. 143–150. ISSN 0572-2691
9. Tsybulkin G. A. The corrective automatic control of trajectory [Korrektırýıýee ýpravlenıe traektornym dvıjenıem] / G. A. Tsybulkin. – Kiev, Stal, 2012. – 161 p. ISBN 978–617–676–011–5
10. Gurskiy A. A. Coordinating automatic control systems of the robot manipulator drivers [Koordınırýıýaıa sıstema avtomatıcheskogo ýpravlenıia prıvodamı robota-manıpýlıatora] / A. A. Gurskiy, A. E. Goncharenko, S. M. Dubna // Automation of technological and business processes. – 2018. – No. 4. – P.11–21. ISBN 2312–3125
11. Air/fuel ratio control in diesel-dual-fuel engine by varying throttle / [W. Chatlatanagulchai, S. Rhienprayoon, K. Yaovaja, K. Wannatong] // EGR valve, and total fuel. – SAE Technical Paper. – 2010. – Issue 2010-01-2200. DOI: https://doi.org/10.4271/2010-01-2200
12. Adaptive air-fuel ratio control scheme and its experimental validations for port-injected spark ignition engines / [Xiaohong Jiao, Jiangyan Zhang, Tielong Shen, Junichi Kako] // International Journal of Adaptive Control and Signal processing. – 2015. – Volume 29, Issue 1. – P. 41–63. DOI: 10.1002/acs.2456.
13. Wong H. Model predictive engine air-ratio control using online sequential relevance vector machine / Hang-cheong Wong, Pak-kin Wong, Chi-man Vong // Journal of Control Science and Engineering. – 2012. – Volume 2012. – P. 2. DOI:10.1155/2012/731825.
14. Decomposition in automatic generation of Petri nets for manufacturing system control and scheduling / [D. W. He, Strege B., Tolle H., Kusiak A.] // International Journal of Production Research – 2000. – Volume 38, Issue 6. – P. 1437–1457. DOI: 10.1080/002075400188942
15. Gurskiy A. A. Tuning of neural network during automatic synthesis of Petri nets (2018) [Nastroıka neıronnoı setı prı avtomatıcheskom sınteze setei Petrı] / A. A. Gurskiy, S. M. Dubna // Automation of technological and business processes. – 2018. – No. 1. – P. 22–32. DOI: https://doi.org/10.15673/atbp.v10i1.877
16. ZENG Ting-jian Analysis and Optimization of Coordination Control System for Ultra Supercritical Power Generation Unit / [Ting-jian ZENG, Zhi-hao LUO, Bo CHEN et al.] // DEStech Transactions on Environment, Energy and Earth Sciences 2017 (ICEPEE 2017). – 2017. – P. 349–352. DOI 10.12783/dteees/icepe2017/11864
17. Miroshnik I. V. Consistent control by multi-channel systems [Soglasovannoe upravlenie mnogokanalnimi sistemami] / I. V. Miroshnik. – Leningrad, Energoatomizdat, 1990. – 128 p. – ISBN 5-283-04476-9.
18. Gurskiy A. Deficiency on the ratio parameters in a control system as a parameter of turbo compressor plant functioning [Nevyazka po sootnosheniyu parametrov v sisteme upravleniya kak pokazatel’ funkcionirovaniya turbokompressornoj ustanovki] / A. A. Gurskiy, A. V. Denisenko, A. E. Goncharenko // Refrigeration Engineering and Technology. – 2014. – No. 4. – P. 58–64. ISSN 0453-8307
19. Coordination control of robot manipulators using flat outputs / [Elisha D. Markus, Hamam Yskander, John T. Agee, Adisa A. Jimoh] // Robotics and Autonomous Systems. – 2016. – Vol. 83. – P. 169–176. https://doi.org/10.1016/ j.robot.2016.05.006
20. Multi-Robot Trajectory Planning and Posi-tion/Force Coordination Control in Complex Welding Tasks / [Yahui Gan, Jinjun Duan, Ming Chen, Xianzhong Dai] // Applied Sciences. – 2019. – 9(5), 924. – P. 23. https://doi.org/10.3390/ app9050924

DOI 10.15588/1607-3274-2020-1-19

UDC 519.816

DECISION-MAKING DURING LIMITED NUMBER OF EXPERIMENTS WITH MULTIPLE CRITERIA

Irodov V. F. – Dr. Sc., Professor, Head of the Department of system analysis and modelling in heat and gas supply, Prydniprovska State Academy of Civil Engineering and Architecture, Dnieper, Ukraine.

Barsuk R. V. – Assistant of the Department of system analysis and modelling in heat and gas supply, Prydniprovska State Academy of Civil Engineering and Architecture, Dnieper, Ukraine.

ABSTRACT

Context. The mechanism of decision-making during limited number of experiments with multiple criteria are considered. The investigation object is process decision-making for project or control in complex systems with multiple criteria.

Objective. It is necessary to determine optimal (most preferred) parameters of the systems with multiple criteria. It is no the mathematical model of the system, there is limited number of experiments only.

Method. A scheme is proposed for constructing a selection mechanism for decision-making in systems with several criteria for which there is a sample of experimental results. The scheme includes the following procedures: an experimental study of a process with several criteria (functions) depending on its parameters; the use of expert evaluation to build a matrix of preferences for individual implementations; building a function of choosing preferred solutions based on a preference matrix by constructing a mathematical model of preference recognition, formulation and solving the problem of generalized mathematical programming as the final step in building the selection mechanism. The decision-making mechanism depends on the expert assessment procedure when comparing a limited set of results with each other, as well as on the statement of conditions when solving the problem of generalized mathematical programming. Comparison of a finite number of experiments is convenient for expert evaluation. Presentation of the final choice as a result of solving the problem of generalized mathematical programming is convenient for using such a mechanism in automatic control systems already without human intervention.

Results. The proposed scheme of decision-making during limited number of experiments has been applied to decision-making of project management for pellet burner. Experimental decision-making results are presented in the presence of several criteria for a pellet burner of a tubular heater, which confirm the acceptability of the developed decision-making mechanism.

Conclusions. It was proposed the new scheme for constructing a selection mechanism for decision-making in systems with several criteria where there is a sample of experimental results only. The scheme of decision-making is includes the solving the problem of generalized mathematical programming as the final step in building the selection mechanism. For the solving the problem of generalized mathematical programming may be applied the evolution search algorithm.

KEYWORDS: decision-making, multiple criteria, function of choosing, generalized mathematical programming.

NOMENCLATURE

A is an ash transfer in time;

$a_1, a_2, \ldots, a_{18}$ are choice function parameters;

x is a set of inlet system parameters;

x^i is a scalar parameters (continuous or discrete);

Ω is the set of admissible parameters;

x_0 is R_S – optimal solution at the set Ω;

x_H is a new solution;

z is a set of outlet system functions (parameters);

z^f is a one from output parameters

R_S is a binary choice relation;

R_G is a fuzzy generation relation;

$S(X)$ is a selection function;

$G(X)$ is a generation function;

$G_H(X)$ is a set of new solutions;

B_{ob} is the table of experimental results;

B is a matching matrix of experimental results;

C is an incomplete choice function;

$\Gamma(x)$ is the choice function;

π is the choice rule;

$R_S^+(x)$ is the upper section to the binary choice relation R_S;

N_{ob} is a number of experiments;

N_b is a number of branches for evolutionary search;

N_E is a number of new solutions (hevristics);

N_{op} is a number of preferred solutions;

S_b is a burner area;

S_{fir} is a useful area for primary air;

L_1 is a primary air flow;

L_{tot} is a total air flow;

X is a subset of parameters;

X_k is a set of preferred solutions according to the binary choice relation R_S at the iterate step k;

k is an iterate step;

X_{k-1} is a set of preferred solutions according to the binary choice relation R_S at the iterate step k–1;

X_{jk} is a set of preferred solutions according to the binary choice relation R_S at the iterate step k for the branch j of evolutionary search;

W is a power of burner.

INTRODUCTION

The basis of the research is an experiment in which the permissible range of parameters determining the state of the system is comprehensively investigated. In each experiment, in addition to the input parameters of the system, the output functions (criteria) of the system under study are measured or calculated. If we confine ourselves only to the experimental sampling of parameters, then it will not be possible to make decisions about the preference of the system parameters over the entire allowable area. It is advisable to build a mathematical model of the

DOI 10.15588/1607-3274-2020-1-20

function of choice, which will allow to extend the rule of preferences of parameters to the entire admissible region. Having an expression for the function of choice, we can formulate and solve the problem of finding the most preferable solutions. The search of the most preferable solutions can be implemented as a result of solving a generalized mathematical programming problem

The object of study is the process of decision-making while developing or managing systems with some parameters. The mathematical model of such a system is used to make decisions for the development or management of systems. The mathematical model of the system can be built on the basis of deductive laws of functioning or on the basis of an experimental study of the system.

The subject of study is the process of decision-making for project or control in complex systems with multiple criteria when information about the system is presented in the form of a limited set of experiment results.

The purpose of the work is to increase the speed the decision-making process for a system with several criteria when setting information about the properties of the system is a set of experimental results.

1 PROBLEM STATEMENT

A system is characterized by a set of parameters $x = \{x^1, x^2, \ldots, x^n\}$, $x \in \Omega$ and a set of output parameters (functions, criteria) $z = \{z^1, z^2, \ldots, z^f\}$. There are training set of experimental results: $B_{ob} = \langle x_q\, y_q \rangle$, $q = 1,2, \ldots, N_{ob}$ and the result of the expert evaluation in the form of the matching matrix $B = \{b_{ij}\}$, $i = 1,2, \ldots, N_{ob}$, $j = 1,2, \ldots, N_{ob}$, which is obtained using expert choice relation R.

It is required to find the choice function C for all set Ω with binary relation R_S such that binary relation R_S corresponds with expert choice relation R.

2 REVIEW OF THE LITERATURE

In the study of certain processes and systems, the goal is often set – to find the "best" values of the parameters of the system under study. Here we will consider such properties of the system that are not formulated using the deductive approach. Then the basis for the study can only be an experiment. As a result of the experiment, an experimental sample of the values of the system parameters and the corresponding values of the functions (criteria) characterizing these states will be obtained.

The traditional approach is to build mathematical models for each function (criterion) separately based on a sample of experimental data. The search for the "best" parameters of the system can be carried out using a set of mathematical models for the criteria. But how to compare several criteria with each other with the traditional approach remains open.

An alternative approach, which is described here, is as follows. The basis of the research is an experiment in which the permissible range of parameters determining the state of the system is comprehensively investigated. In each experiment, in addition to the input parameters of the system, the output functions (criteria) of the system under study are measured or calculated. If we confine ourselves only to the experimental sampling of parameters, then it will not be possible to make decisions about the preference of the system parameters over the entire allowable area.

It is advisable to build a mathematical model of the function of choice, which will allow "to extend" the rule of preferences of parameters to the entire admissible region. Having an expression for the function of choice, we can formulate and solve the problem of finding the most preferable solutions.

To date, there is sufficient experience in using binary relations of choice in constructing a mechanism for choosing decisions, in particular, scientific results [1–4] and other.

If there is a system that does not have a reliable mathematical model based on deductive laws of functioning, then the inductive principles of mathematical modelling of such systems are known [5, 6] that have received significant development. In inductive modelling, various mathematical models were constructed from experimental data. In this case, it is possible to build functional dependencies for each of several output functions of the system. Having mathematical dependencies for several output functions, you can solve the decision problem as a multi-objective optimization problem. There is a fairly large number of scientific results in the field of multi-optimized optimization [7–10].

Most of these results relate to the situation where there are mathematical models for each of the output functions – Pareto optimization. In this case, the adoption of the final decision from the set of Pareto-optimal is an additional procedure.

An alternative approach is the formulation of an optimization problem as an optimization task with respect to choice relation. Previously, generalized mathematical programming problems were formulated for which solution methods were proposed [11, 12] and other. Later works are also devoted to solving the problem of generalized mathematical programming, for example [13].

Effective methods for solving optimization problems are developed on the basis of evolutionary search algorithms, for example, [14–16]. Including evolutionary algorithms useful for solving problems of generalized mathematical programming [16, 17] without the convexity condition of choice relation.

Previously, it was not offered a general scheme for constructing a selection mechanism for decision-making in systems with several criteria where there is a sample of experimental results only. The scheme of decision-making is includes the solving the problem of generalized mathematical programming as the final step in building the selection mechanism. For the solving the problem of generalized mathematical programming may be applied the evolution search algorithm.

MATERIALS AND METHODS

Let a system be considered whose state is characterized by a set of parameters $x = \{x^1, x^2, \ldots, x^n\}$. Each system

DOI 10.15588/1607-3274-2020-1-20

state is characterized by a set of output parameters (functions, criteria) $z = \{z^1, z^2, ..., z^f\}$.

We assume that as a result of the experiments, a training set of experimental results was obtained: $B_{ob} = <x_q\ y_q>$, $q = 1,2, ..., N_{ob}$. In terminology of the theory of decision making [2–4], a separate result of the sample will be called presentation. We assume that the set of presentations of the training sample B_{ob} by expert evaluation taking into account the values of output functions for any pair of presentations, a binary relation R_S: $x_i\ R_S\ x_j$ for $i,j = 1,2, ..., N_{ob}$ is established. The result of the expert evaluation for the comparison of the presentations with each other will be represented in the form of the matching matrix $B = \{b_{ij}\}$, $i = 1,2, ..., N_{ob}$, $j = 1,2, ..., N_{ob}$, where

$$\begin{cases} b_{ij} = 1, \text{ if } x_i R x_j, \\ b_{ij} = 0, \text{ if } x_j R x_i. \end{cases}$$

We will search for the selection rule π with the selection function

$$S(X) = \left\{x \in X \middle| \forall y \in [X \setminus S(X)], xR_S y\right\}.$$

and the binary relation R_S, which is determined by the function $\Gamma(x) = \Gamma(x^1, x^2, \ldots, x^n)$, such that

$$\Gamma(x_1) \geq \Gamma(x_2) \equiv x_1\ R_S\ x_2.$$

where $x_1 \in \Omega$, $x_2 \in \Omega$.

The function $\Gamma(x)$ is defined on the whole set of admissible parameters Ω and the binary relation R_S is defined for all pairs of elements from Ω, and not just for pairs of elements from the set of experimental results.

In this sense, we can talk about the problem of approximation [4]. The function $\Gamma(x)$ and the binary relation R_S should be determined from the condition of the best fit to the matrix $B = \{b_{ij}\}$, $i = 1,2, ..., N_o$, $j = 1,2, ..., N_o$ for comparison of objects according to the results of experiments.

The binary relation R_S with the choice function obtained in this way can be used to search for the most preferable solutions on the entire Ω set, taking into account possible limitations as well.

Following the terminology of [2], the choice rule is a rule, according to which there can be an by element or integral definition of the choice function:

$$\pi:\ y \in X \mid \ldots$$

$$\pi:\ Y \subseteq X \mid \ldots$$

In these formulas, instead of the ellipsis, one or another record of the corresponding conditions, which characterize the choice rule, is meant.

The task of the synthesis [2] is to construct a mechanism of choice that implements this function based on the function of the (incomplete) choice C, or to establish that it cannot be done. The function C, for which the synthesis problem is solved, can describe the experimentally observed choice.

The article aims to offer a rational scheme for making the most preferable solutions for researching a system with several criteria, ranging from experimental research of the system and obtaining a sample of experimental data, ending with the formulation and solution of the problem of finding the most preferred parameters as a generalized mathematical programming problem.

To achieve this goal, it was necessary to develop a method for constructing a function of choice, based on a sample of experiments, and then to extend the function of choice to the whole admissible region. In addition, it was necessary to develop or choose from previously developed such a method for solving the problem of generalized mathematical programming, which will allow to provide a final search for the most preferable solution on the permissible parameter area in the presence of constraints.

The methods for solving the problems are based on the approach to the evolutionary search for R_S – optimal solutions. For subset X, $X \subset \Omega$ we denote the function of choice in the form

$$S(X) = \left\{x \in X \middle| \forall y \in [X \setminus S(X)], xR_S y\right\}. \quad (1)$$

We shall assume that set $S(X)$ contains the concrete number of elements – N_{op}.

We shall that for the set Ω it was determined relation R_G with attachment function $\mu_{R_G}(x, y)$: $\Omega \times \Omega \to [0,1]$. Relation R_G will be termed generation relation.

For subset X, $X \subset \Omega$ we denote the function of generation in the form

$$G(X) = X \cup G_H(X),$$

$$G_H(X) = \left\{y \in \Omega \middle| \exists x \in X, yR_G x, \mu_{R_G}(x, y) > 0\right\}. \quad (2)$$

We shall assume that set $G(X)$ contains the concrete number of elements – N_E.

The algorithm to search R_S –optimal solution can be represented as

$$X_k = S(G(X_{k-1})),\ k = 1,2,... \quad (3)$$

The iterate algorithm (3) – is the general form of evolutionary search.

According to [15–17] we will consider the decomposition

$$X_k = \bigcup_{j=1}^{N_b} X_{jk}\ ,\ X_{ik} \cap X_{jk} = \varnothing\ ,\ i \neq j\ . \quad (4)$$

The algorithm (3) takes the form

$$X_{jk} = S(G(X_{jk-1})),\ j = \overline{1, N_b}\ ,\ k = 1,2,... \quad (5)$$

These iterate algorithms (3), (5) – are the general form of evolutionary search.

We denote by $R_S^+(x)$ the upper section to the binary choice relation R_S at the set Ω:

$$R_S^+(x) = \left\{y \in \Omega \middle| yR_S x\right\}. \quad (6)$$

We will assume that upper sections have such properties:

$$\forall x \neq x_0\ \ mes R_S^+(x) > 0. \quad (7)$$

Relatively of generation function we will consider following. If x_H is a new solution $x_H \in G_H(X)$, then

$$\forall x \neq x_0\ \ P\left\{x_H \in R_S^+(x)\right\} \geq \delta > 0. \quad (8)$$

DOI 10.15588/1607-3274-2020-1-20

Convergence of the sequence X_k to R_S –optimal solution we understand the following. For every $x \in \Omega$, $x \neq x_0$ there is a number K that for each $k \geq K$ with probability 1 that will be satisfied:

$$X_K \subset R_S^+(x).$$

The following theorem [13] holds:

If upper sections (6) have the property (7), generation function (2) has the property (8), and choice relation R_S is a no strictly order relation, then algorithm (3) ensures convergence of the sequence X_k to R_S – optimal solution with probability 1.

Analogically [16] this theorem can be extended for all branches of evolutionary search (5).

4 EXPERIMENTS

There are considered tubular gas heater [18]. Tubular heaters design parameters (inlet system parameters) are below:

– Burner area, S_b;
– Useful area for primary air passage, S_{fir};
– Primary air flow, L_1;
– Total air flow, L_{tot};
– Burner power, W.

There are criteria (outlet system functions) of the heater:

– Ash transfer by the time, A;
– Concentration CO at exhaust gases, C_{CO};
– Concentration NO_x at exhaust gases, C_{NOx}.

There are following requirements for parameters that characterize tubular heaters work: for CO it is less than 130 mg/m^3 and for NO_x – less than 250 mg/m^3. Therefore such tags as CO and NO_x are shown at tubular heater schematically block diagram. Also such parameter as ash is typical because of strengthened primary air supply creates unintended carrying out ash from the burner. It leads to tube clogging, which degrades heat transfer and reduces tube efficiency time.

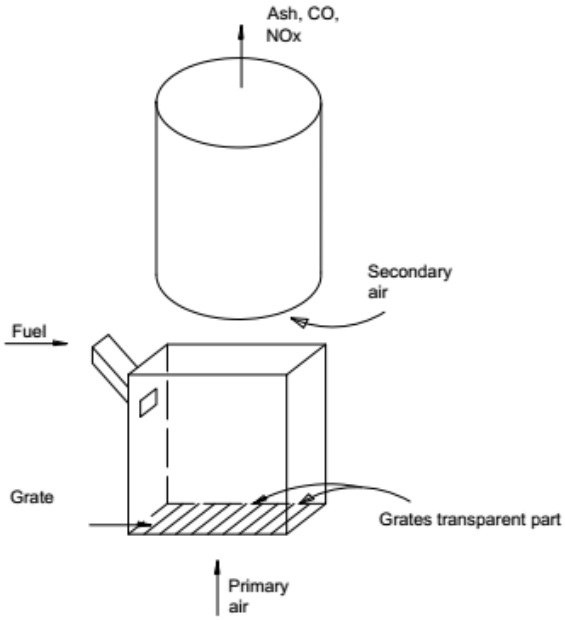


Figure 1 – Tubular heater pellets burner principle diagram

Experimental results are presented in two arrays: array 1 (Table 1) and array 2 (Table 2).

After expert evaluation of array 1 (Table 1) and array 2 (Table 2), matching matrixes B were obtained – Table 3 and Table 4.

Table 1 – Experimental data array1

							max=130	max=250
№	S	S пер	$L_{заг}$	L_1	W	З	C_{CO}	C_{NOx}
1	0.5	0.572	0.7155	0.440252	0.335	0.175	0.012	0.964
2	0.5	0.572	0.6795	0.430464	0.313	0.240	0.153	0.681
3	0.5	0.572	0.6795	0.397	0.547	0.231	0.001	0.852
4	1	0.643	0.792	0.738	0.18	0.018	0.102	0.845
5	1	0.643	0.8145	0.828	0.32	0.039	0.016	0.674
6	1	0.643	0.855	0.736	0.355	0.458	0.003	0.757
7	1	0.643	0.7785	0.924	0.828	0.233	–	–
8	0.5	0.254	0.8865	0.38	0.26	0.024	–	–
9	0.5	0.245	0.7425	0.484	0.32	0.018	–	–
10	0.5	0.254	0.7515	0.509	0.36	0.010	–	–
11	1	0.287	0.819	0.769	0.3	0.083	–	–
12	1	0.287	0.774	0.872	0.6	0.278	–	–
13	1	0.287	0.742	0.787	0.94	0.202	–	–
14	0.5	0.572	0.723	0.218	0.18	–	0.051	0.431
15	0.5	0.572	0.671	0.134	0.2	–	0.016	0.753
16	0.25	0.084	0.25125	0.134	0.064	0.298	0.063	0.293
17	0.25	0.084	0.21	0.244	0.09	0.583	0.066	0.441
18	0.25	0.084	0.20625	0.26	0.18	0.833	0.164	0.359
19	0.25	0.084	0.188	0.337	0.18	0.583	0.178	0.411
20	0.25	0.084	0.268	0.102	0.047	0.133	0.032	0.48
21	0.25	0.084	0.25125	0.139	0.113	0.408	0.03	0.635
22	0.25	0.084	0.245	0.153	0.1	0.417	0.023	0.691
23	0.25	0.084	0.2275	0.214	0.128	0.300	0.018	0.697
24	0.25	0.084	0.2225	0.14	0.053	0.150	0.018	0.661
25	0.25	0.084	0.208	0.167	0.045	0.058	0.049	0.526

DOI 10.15588/1607-3274-2020-1-20

Table 2 – Experimental data array 2

							max=130	max=250
№ (cont.)	S	S пер	$L_{заг}$	L_1	W	З	C_{CO}	C_{NOx}
26	0.25	0.084	0.194	0.194	0.06	0.142	0.016	0.872
27	0.25	0.084	0.187	0.233	0.112	0.233	0.014	0.852
28	0.25	0.084	0.175	0.285	0.18	0.450	0.026	0.789
29	0.25	0.084	0.17	0.33	0.225	0.875	0.019	0.845
30	0.25	0.084	0.16	0.546	0.225	0.942	0.018	0.859
31	0.25	0.084	0.158	0.197	0.082	0.158	0.025	0.441
32	0.25	0.084	0.15375	0.2439	0.09	0.083	0.010	0.618
33	0.25	0.084	0.13875	0.306	0.113	0.158	0.006	0.497
34	0.25	0.084	0.131	0.362	0.15	0.250	0.01	0.625
35	0.25	0.084	0.121	0.422	0.15	0.400	0.028	0.783
36	0.25	0.084	0.106	0.588	0.225	0.858	0.019	0.668
37	0.25	0.084	0.1	0.8125	0.18	0.900	0.021	0.714
38	0.25	0.084	0.2625	0.13	0.039	0.108	0.067	0.53
39	0.25	0.084	0.21875	0.234	0.09	0.283	0.151	0.184
40	0.25	0.084	0.215	0.25	0.075	0.467	0.065	0.487
41	0.25	0.084	0.21	0.303	0.18	0.292	0.045	0.431
42	0.25	0.084	0.19	0.145	0.05	0.417	0.042	0.382
43	0.25	0.084	0.186	0.188	0.075	0.333	1	1
44	0.25	0.084	0.18875	0.198	0.113	0.317	0.09	0.26

Table 3 – Matching matrix for experimental data array 1

DATA 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,1,1,1,1,1,1
DATA 0,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,0,0,1,1,1,1,1,1
DATA 0,0,1,0,0,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0
DATA 0,1,1,1,0,1,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,1,1,1,1,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,0,1,1,0,1,1,1,1,0,0,1,0,0,0,0,0,0,0,0,0,0,1
DATA 0,0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
DATA 0,0,0,1,1,0,1,1,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0
DATA 0,0,1,1,1,0,1,1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0,0
DATA 0,0,0,1,1,0,0,1,1,1,0,0,1,0,1,0,0,0,0,0,0,0,0,0
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,1,1,1,1,1
DATA 0,0,1,0,1,1,1,1,1,1,1,1,0,0,0,0,1,0,0,0,0,0,0,0,0
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,1,1,1,1,1
DATA 1,0,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,1,1,1,1,1
DATA 1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,1,1,1,1,1,1
DATA 1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,0,1,0,0,0,0,1,0,1,1,1,0
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,0,1,0,0,0,0,1,1,1,1,1,0
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,1,1,1,0
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0,1,0,1
DATA 0,0,1,0,1,1,1,1,1,1,1,1,1,0,1,0,0,0,0,0,0,0,1,1,0
DATA 0,0,1,0,1,1,0,1,1,1,1,1,1,0,1,0,0,0,0,1,1,1,0,1,1

Table 4 – Matching matrix for experimental data array 2

DATA 1,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1
DATA 1,1,0,1,1,1,1,1,0,0,0,1,1,1,1,1,1,1,1,1,1
DATA 1,1,1,1,1,1,1,1,0,0,0,1,1,1,0,1,1,1,0,1,1
DATA 1,0,0,1,0,1,0,0,0,0,0,0,1,1,1,1,1,0,1,1
DATA 1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1
DATA 1,0,0,0,1,1,1,1,1,0,0,1,1,0,0,0,0,0,0,1,1
DATA 1,0,0,1,1,0,1,0,0,0,0,0,1,1,1,1,1,1,1,1,1
DATA 1,1,1,1,1,0,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1
DATA 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1
DATA 1,1,1,1,1,1,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1
DATA 1,0,0,1,1,0,1,0,0,0,1,0,0,0,0,0,0,0,1,1,1
DATA 1,0,0,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,1
DATA 1,0,0,0,1,1,0,0,0,0,0,1,1,1,1,0,1,0,0,0,1,1
DATA 1,0,1,0,1,1,0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,1
DATA 0,0,0,0,0,1,0,0,0,0,1,1,0,0,1,0,0,0,0,1,1
DATA 1,0,0,0,1,1,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1
DATA 1,0,0,0,1,1,0,0,0,0,1,1,1,0,1,0,1,0,1,0,1,0
DATA 1,0,1,1,1,1,0,0,0,0,1,1,1,0,1,0,1,1,1,1,0
DATA 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0

DOI 10.15588/1607-3274-2020-1-20

5 RESULTS

There are presented results with choice function in the form (9).

$$\begin{aligned} &\Gamma(x) = d_1+d_2+d_3,\\ &d_1= (a_1+a_2x^1 +a_3x^1x^1) (a_4+a_5x^2 +a_6x^2x^2),\\ &d_2=(a_7+a_8x^3 +a_9x^3x^3) (a_{10}+a_{11}x^4 +a_{12}x^4x^4),\\ &d_3=(a_{13}+a_{14}x^4 +a_{15}x^4x^4) (a_{16}+a_{17}x^5 +a_{18}x^5x^5),\\ &\Gamma(x_1)\geq \Gamma(x_2)\equiv x_1 R_S x_2. \end{aligned} \quad (9)$$

Parameters a_1, a_2 ,…, a_{18} were obtained after evolutionary search the choice function for array 1 of experimental data and for array 2 of experimental data.

The choice function in the form (19) with specific values of parameters a_1, a_2 ,…, a_{18} was used to solve the problem of generalized mathematical programming: to find maximum choice function with restrictions: $0.2<=x^i=<0.5$, $i=1,\ldots,5$. Evolutionary search for solving the problem of generalized mathematical programming is illustrated at tabl. 6 and results of evolutionary search for three branches of evolution are presented in Table 7.

6 DISCUSSION

It is advisable to discuss the stated decision-making mechanism. The first stage of the decision-making mechanism is the experimental study of the system. When conducting experiments, it is desirable to examine as widely as possible the allowable input parameters $x= \{x_1, x_2,\ldots, x_n\}$. It does not require the use of experimental planning methods. The tables of experimental results are a typical example. A visual analysis of the experimental results shows the existence of interdependencies of the output parameters (functions) among themselves.

The controversial nature of the mutual influence of output parameters is clearly seen. Matrix of conformity (Table 3 and Table 4) is the result of expert assessment and is subjective. For expert assessment, it is obviously possible to use the whole variety of available pair-wise comparison methods and use a different scale for such an assessment. The choice function given in the article in the form of an algebraic function is certainly not the only possible one, here you can use the whole variety of pattern recognition methods, for example [19, 20].

An important property of such a function is the reliability of the reflection of experimental results not only for the training sequence, but also for the checking sequence of experimental results. The use of an evolutionary search algorithm with several branches of evolution is convenient for controlling the found solution. For example, from Table 6 it can be seen that as a result of the search, the value of the choice function reached a maximum (one) in all three branches of the evolution of solutions. The values of the parameters are basically the same, although there is a slight discrepancy in some parameters.

This suggests that the maximum of this choice function is poorly defined. If in the search process there was no convergence of results across different branches of evolution, this would indicate the absence of a single solution. In this example, the solutions found for the three branches of evolution are almost identical, which indicates the presence of a global maximum of the choice function.

Table 5 – Evolutionary search the choice function

Iteration step of evolutionary search	Error at the training array 1	Error at the test array 2
1	0.2912	0.3975
2	0.2656	0.4425
6	0.2464	0.2675
10	0.2400	0.2675
14	0.2336	0.2675
18	0.2240	0.2675
27	0.1856	0.2675
38	0.1664	0.2525
96	0.1536	0.2575
214	0.1440	0.2575

Table 6 – Evolutionary search for solving the problem of generalized mathematical programming

Iteration step of evolution	Maximum function Branch 1 of evolution	Maximum function Branch 2 of evolution	Maximum function Branch 3 of evolution
1	–1.47E–7	–1.57E–7	–1.30E–7
2	8.45E–7	–1.28E–7	7.65E–7
5	1.53E–6	5.02E–6	4.78E–5
11	0.202	0.185	0.111
14	0.9950	0.9993	0.9953
15	0.9996	1	0.9975
16	1	1	0.9981
17	1	1	0.9985
18	1	1	0.9999
19	1	1	0.9999
20	1	1	1

Table 7 – Result of evolutionary search for solving the problem of generalized mathematical programming

Branches of evolution	Parameter 1 x^1	Parameter 2 x^2	Parameter 3 x^3	Parameter 4 x^4	Parameter 5 x^5
Branch 1	0.3800	0.5	0.2	0.4511911	0.2
Branch 2	0.4080	0.5	0.2	0.4511911	0.2
Branch 3	0.3949	0.5	0.2	0.4511911	0.2020

DOI 10.15588/1607-3274-2020-1-20

CONCLUSIONS

The constructed selection function is determined already on the whole admissible space of input parameters, and not only on the set of experimental points.

Thus, the selection mechanism extends to the entire allowable range of input parameters.

The scheme includes the following procedures: an experimental study of a process with several criteria (functions) depending on its parameters; the use of expert evaluation to build a matrix of preferences for individual implementations; building a function of choosing preferred solutions based on a preference matrix by constructing a mathematical model of preference recognition, formulation and solving the problem of generalized mathematical programming as the final step in building the selection mechanism.

The scientific novelty is result presented as a holistic decision-making mechanism for a system based on inductive modeling of complex systems, in which the following steps can be distinguished: an experimental study of a process with several criteria (functions) depending on its parameters; the use of expert evaluation to build a matrix of preferences for individual implementations; building a function of choosing preferred solutions based on a preference matrix by constructing a mathematical model of preference recognition, formulation and solving the problem of generalized mathematical programming as the final step in building the selection mechanism.

The practical significance of obtained results is that the stated decision-making mechanism can be used for a wide range of complex systems with several criteria.

Prospects for further research are to the improvement of methods and means for constructing a function of choice for a limited number of experimental results.

ACKNOWLEDGEMENTS

This work was carried out within the framework of the budget research work of the Pridneprovska State Academy of Civil Engineering and Architecture (state registration number 0112U005350).

REFERENCES

1. Fishburn P. Representiable choice function, *Econometrica,* 1976, Vol. 44, No. 5, pp. 1033–1043.
2. Ajzerman M. A., Aleskerov F. T. Vibor variantov: osnovi teorii. Moscow, Nauka, 1990, 240 p. ISBN 5-02-014091-0.
3. Ajzerman M.A. Nekotorie novie zadachi obchej teorii vibora (obzor odnogo napravleniya issledovaniy), *Avtomat. i telemeh.*, 1984, No. 9, pp. 5–43.
4. Sholomov L.A. Logicheskie metodi postroeniya i analiza modeley vibora. Moscow, Nauka, 1989, 288 p. ISBN 5-02-014108-9.
5. Ivakhnenko A.G. Heuristic Self-Organization in Problems of Engineering Cybernetics, *Automatica*, 1970, Vol. 6, pp. 207–219.
6. Ivakhnenko A.G. Polynomial Theory of Complex Systems, *IEEE Transactions on Systems Man and Cybernetics*, 1971, Vol. 4, pp. 364–378.
7. Lemarchand L., Masse D., Rebreyend P., Hakansson J. Multiobjective optimization for multimode transportation problems, *Advances in Operations Research*, 2018, Vol. 2018, 13 p. https:// doi.org/10.1155/2018/8720643.
8. Sagawa M., Kusuno N., Aguirre H., Tanaka K., Koishi M. Evolutionary multiobjective optimization including practically desirable solutions, *Advances in Operations Research, Article ID 9094514*, 2017, Vol. 2017, 16 p. https:// doi.org/10.1155/2017/9094514.
9. Giagkiozis I., Fleming P. J. Pareto front estimation for decision making, *Evolutionary computation*, 2014, Vol. 22, No. 4, pp. 651–678. htts: //www.researchgate/publication/261369702.
10. Wang Y., Sun X. A many-objective optimization algorithm based on weight vector adjustment, *Computational Intelligence and Neuroscience,* 2018, Vol. 2018, Article ID 4527968, 21 p. DOI: 10.1155/2018/4527968.
11. Yudin D. B. Generalized mathematical programming, *Economics and Mathematical Methods,* 1984, Vol. 20, pp. 148–167.
12. Judin D.B. Vichislitelnie metodi teorii prinyatiya resheniy / D.B. Judin. – M. : Nauka, 1989. – 320 p.
13. Kolbin V. V. Generalized mathematical programming as a decision model, *Applied Mathematical Sciencies,* 2014, Vol. 8, No. 70, pp. 3469–3476. DOI 10.12988/ams.2014.44231.
14. Irodov V. F., Maksimenkov V. P. Application of an evolutionary program for solving the travelling-salesman problem, *Sov. Autom. Control ; translation from Avtomatika,* 1981, No. 4, pp. 7–10. io-port.net Database 03803175.
15. Irodov V. F. The construction and convergence of evolutional algorithms of random search for self-organization, *Sov. J. Autom. Inf. Sci. 20 ; translation from Avtomatika*, 1987, No.4, pp. 34–43. io-port.net Database 04072731.
16. Irodov V. F. Self-organization methods for analysis of nonlinear systems with binary choice relations, *System Analysis Modeling Simulation*, 1995, Vol. 18–19, pp. 203–206. https://dl.acm.org/citation.cfm?id=208028#.
17. Irodov V. F., Khatskevych Yu. V. Convergence of evolutionary algorithms for optimal solution with binary choice relations, *Stroitelstvo, materialovedenie, mashinostroenie : Sb. nauch. trudov.* Dnepr, 2017, Vol. 98, pp. 91–96. http://nbuv.gov.ua/UJRN/smmeect_2017_98_16.
18. Barsuk R. V., Irodov V. F. Matematichne modeliuvannya funkcii viboru perevazhnih rishen dlya trubchastih gazovih nagrivachiv za eksperimentalnoiy informazieiy, *Visnik Pridneprovskoi derzhavnoi akademii budivniztva ta architecturi : zb. nauk. prats.* Dnipro, 2016, No. 8(221), pp. 17–25. http://oaji.net/articles/2017/2528-1507122475.
19. Subbotin S. A. The neuro-fuzzy network synthesis and simplification on precedents in problems of diagnosis and pattern recognition, *Optical Memory and Neural Networks (Information Optics)*, 2013, Vol. 22, No. 2, pp. 97–103. DOI: 10.3103/s1060992x13020082.
20. Subbotin S. A. Methods of sampling based on exhaustive and evolutionary search, *Automatic Control and Computer Sciences,* 2013, Vol. 47, No. 3, pp. 113–121. DOI: 10.3103/s0146411613030073.

Received 15.01.2019.
Accepted 23.02.2020.

DOI 10.15588/1607-3274-2020-1-20

УДК 519.816

ПРИЙНЯТТЯ РІШЕНЬ ПРИ НАЯВНОСТІ ОБМЕЖЕНОГО ЧИСЛА ЕКСПЕРИМЕНТІВ З ДЕКІЛЬКОМА КРИТЕРІЯМИ

Іродов В. Ф. – д-р техн. наук, професор, завідувач кафедри системного аналізу та моделювання у теплогазопостачанні Придніпровської державної академії будівництва та архітектури, Дніпро, Україна.

Барсук Р. В. – асистент кафедри системного аналізу та моделювання у теплогазопостачанні Придніпровської державної академії будівництва та архітектури, Дніпро, Україна.

АНОТАЦІЯ

Актуальність. Розглянуто задачу прийняття рішень для системи з декількома критеріями на основі обмеженої кількості експериментальних результатів. Об'єктом дослідження є процес прийняття рішень, починаючи з експериментального дослідження системи до рішення задачі оптимізації системи з декількома критеріями.

Мета. Мета роботи – викладення цільного механізму прийняття рішень для системи з декількома критеріями на основі обмеженої кількості експериментів.

Метод. Запропоновано використовувати алгоритми еволюційного пошуку переважних рішень для двох основних процедур: пошук оптимальної функції вибору на базі матриці пере важності експериментальних рішень; пошук оптимальних по бінарному відношенню вибору рішень на всій множині допустимих параметрів (рішення задачі узагальненого математичного програмування). Алгоритм еволюційного пошуку, який застосовується, вирішує задачу пошуку оптимальних по бінарному відношенню вибору рішень без потреби випуклості відношення вибору. У роботі застосовані експериментальні результати дослідження пальника на паливних гранулах (пелетах). Вхідні параметри системи налічують п'ять розмірних параметрів, а вихідні параметри три розмірні критерії. Усього експерименти налічують 45 результатів, з яких 25 експериментів склали навчальну послідовність і 20 результатів – контрольну послідовність, які застосовувались для отримання функції вибору.

Результати. Розроблена цільна система побудови механізму прийняття рішень для системи з декількома критеріями на основі обмеженої кількості експериментів.

Висновки. Наведені експерименти та їх обробка показали достовірність основних наукових результатів – можливості побудови механізму вибору у системі з декількома критеріями на основі обмеженої кількості експериментів і поширення кінцевого вибору на всю допустиму область вхідних параметрів, а не тільки на множині експериментальних результатів.

КЛЮЧОВІ СЛОВА: механізм прийняття рішень, декілька критеріїв, функція вибору, узагальнено математичне програмування.

УДК 519.816

ПРИНЯТИЕ РЕШЕНИЙ ПРИ НАЛИЧИИ ОГРАНИЧЕННОГО КОЛИЧЕСТВА ЭКСПЕРИМЕНТОВ С НЕСКОЛЬКИМИ КРИТЕРИЯМИ

Иродов В. Ф. – д-р техн. наук, профессор, заведующий кафедрой системного анализа и моделирования в теплогазоснабжении Приднепровской государственной академии строительства и архитектуры, Днепр, Украина.

Барсук Р. В. – ассистент кафедры системного анализа и моделирования в теплогазоснабжении Приднепровской государственной академии строительства и архитектуры, Днепр, Украина.

АННОТАЦИЯ

Актуальность. Рассмотрена задача принятия решений для системы с несколькими критериям на основе ограниченного количества экспериментальных результатов. Объектом исследования является процесс принятия решений, начиная с экспериментального исследования системы к решению задачи оптимизации системы с несколькими критериями.

Цель. Цель работы – изложение цельного механизма принятия решений для системы с несколькими критериям на основе ограниченного количества экспериментов

Метод. Предложено использовать алгоритмы эволюционного поиска предпочтительных решений для двух основных процедур: поиск оптимальной функции выбора на базе матрицы предпочтительности экспериментальных решений; поиск оптимальных по бинарному отношению выбора решений на всем множестве допустимых параметров (решение задачи обобщенного математического программирования). Алгоритм эволюционного поиска, который применяется, решает задачу поиска оптимальных по бинарному отношению выбора решений без требования выпуклости отношение выбора. В работе применены экспериментальные результаты исследования горелки на топливных гранулах (пеллетах). Входные параметры системы насчитывают пять размерных параметров, а выходные параметры три размерные критерии. Всего эксперименты насчитывают 45 результатов, из которых 25 экспериментов составили учебную последовательность и 20 результатов – контрольную последовательность, которые применялись для получения функции выбора.

Результаты. Разработана цельная система построения механизма принятия решений для системы с несколькими критериям на основе ограниченного количества экспериментов.

Выводы. Приведенные эксперименты и их обработка показали достоверность основных научных результатов – возможности построения механизма выбора в системе с несколькими критериям на основе ограниченного количества экспериментов и распространения конечного выбора на всю допустимую область входных параметров, а не только на множестве экспериментальных результатов.

КЛЮЧЕВЫЕ СЛОВА: механизм принятия решений, несколько критериев, функция выбора, обобщенное математическое программирование.

DOI 10.15588/1607-3274-2020-1-20

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Fishburn P. Representiable choice function / P. Fishburn // Econometrica. – 1976. – Vol. 44, № 5. – P. 1033–1043.
2. Айзерман М.А. Выбор вариантов : основы теории / М. А. Айзерман, Ф.Т. Алескеров. – М. : Наука, Гл. ред. физ.-мат. лит., 1990. – 240 с. – ISBN 5-02-014091-0.
3. Айзерман М.А. Некоторые новые задачи общей теории выбора (обзор одного направления исследований) / М. А. Айзерман // Автомат. и телемех. – 1984. – № 9. – С. 5–43.
4. Шоломов Л. А. Логические методы построения и анализа моделей выбора / Л. А. Шоломов. – М. : Наука, 1989. – 288 с.– ISBN 5-02-014108-9.
5. Ivakhnenko A.G. Heuristic Self-Organization in Problems of Engineering Cybernetics / A.G. Ivakhnenko // Automatica. – 1970. – Vol. 6. –P. 207–219.
6. Ivakhnenko A.G. Polynomial Theory of Complex Systems / A.G. Ivakhnenko // IEEE Transactions on Systems Man and Cybernetics. – 1971. – Vol. 4. – P. 364–378.
7. Lemarchand L. Multiobjective optimization for multimode transportation problems / L. Lemarchand, D. Masse, P. Rebreyend, J. Hakansson // Advances in Operations Research. – 2018. – Vol. 2018. – 13 p. https:// doi.org/10.1155/2018/8720643.
8. Sagawa M. Evolutionary multiobjective optimization including practically desirable solutions / M. Sagawa, N. Kusuno, H. Aguirre, K. Tanaka, M. Koishi // Advances in Operations Research, Article ID 9094514. – 2017. – Vol. 2017, 16 p. https:// doi.org/10.1155/2017/9094514.
9. Giagkiozis I. Pareto front estimation for decision making / I. Giagkiozis, P. J. Fleming // Evolutionary computation. – 2014. – Vol. 22, № 4. – P. 651–678. htts: //www.researchgate/publication/261369702.
10. Wang Y. A many-objective optimization algorithm based on weight vector adjustment / Y. Wang, X. Sun // Computational Intelligence and Neuroscience. – 2018. – Vol. 2018, Article ID 4527968, 21 p. DOI: 10.1155/2018/4527968.
11. Yudin D.B. Generalized mathematical programming / D. B. Yudin // Economics and Mathematical Methods. – 1984. – Vol. 20. – P. 148–167.
12. Юдин Д. Б. Вычислительные методы теории принятия решений / Д. Б. Юдин. – М. : Наука, 1989. – 320 с.
13. Kolbin V. V. Generalized mathematical programming as a decision model / V. V. Kolbin // Applied Mathematical Sciencies. – 2014. – Vol. 8, № 70. – P. 3469–3476. DOI 10.12988/ams.2014.44231.
14. Irodov V. F. Application of an evolutionary program for solving the travelling-salesman problem / V.F. Irodov, V. P. Maksimenkov // Sov. Autom. Control ; translation from Avtomatika. – 1981. – № 4. – P. 7–10. io-port.net Database 03803175.
15. Irodov V. F. The construction and convergence of evolutional algorithms of random search for self-organization / V.F. Irodov // Sov. J. Autom. Inf. Sci. 20 ; translation from Avtomatika. – 1987. – № 4. – P. 34–43. io-port.net Database 04072731.
16. Irodov V. F. Self-organization methods for analysis of nonlinear systems with binary choice relations / V. F. Irodov // System Analysis Modeling Simulation. – 1995. – Vol. 18–19. – P. 203–206. https://dl.acm.org/citation.cfm?id=208028#.
17. Irodov V. F. Convergence of evolutionary algorithms for optimal solution with binary choice relations / V. F. Irodov, Yu. V. Khatskevych // Строительство. Материаловедение. Машиностроение : сб. науч. тр. / Приднепров. гос. акад. стр-ва и архитектуры. – Дн-вск, 2017. – Вып. 98. – С. 91–96. – (Серия: Энергетика, экология, компьтерные технологии в строительстве). http://nbuv.gov.ua/UJRN/smmeect_2017_98_16.
18. Барсук Р. В. Математичне моделювання функції выбору переважних рішень для трубчастих газових нагрівачів за експериментальної інформації / Р. В. Барсук, В. Ф. Іродов // Вісник Придніпровської державної академії будівництва та архітектури : зб. наук. пр. / Придніпров. держ. акад. буд-ва та архітектури. – Дніпропетровськ, 2016. – №8(221). – С. 17–25. http://oaji.net/articles/2017/2528-1507122475.
19. Subbotin S. A. The neuro-fuzzy network synthesis and simplification on precedents in problems of diagnosis and pattern recognition / S. A. Subbotin // Optical Memory and Neural Networks (Information Optics). – 2013. – Vol. 22, № 2. – P. 97–103. DOI: 10.3103/s1060992x13020082.
20. Subbotin S. A. Methods of sampling based on exhaustive and evolutionary search / S. A. Subbotin // Automatic Control and Computer Sciences. – 2013. – Vol. 47, № 3. – P. 113–121. DOI: 10.3103/s0146411613030073.

DOI 10.15588/1607-3274-2020-1-20

UDC 621.51

METHOD OF UNCERTAIN COEFFICIENTS IN PROBLEMS OF OPTIMAL STABILIZATION OF TECHNOLOGICAL PROCESSES

Stenin A. A. – Dr. Sc., Professor of the Department of technical Cybernetics, Igor Sikorsky Kyiv Polytechnic Institute, Kiev, Ukraine.

Drozdovich I. G. – Senior researcher, Institute of telecommunications and global information space of NAS of Ukraine, Kiev, Ukraine.

Soldatova M. A. – Senior lecturer of the Department of automated information processing and management systems, Igor Sikorsky Kyiv Polytechnic Institute, Kiev, Ukraine.

ABSTRACT

Context. The equivalent transformation method is examined in the given article. Its essence lies in changing of a certain class of non-stationary systems with the stationary ones, for which optimization methods are well processed. Urgency of the method is determined by the fact that in most optimal control methods, developed for continuous systems, tasks are considered in the temporary space using the states space and the matrix theory. All real control objects are known to be non-linear and non-stationary in one way or another. Analysis and synthesis of control systems for such objects is a complex mathematical issue, and its solution is received for some separate occasions for now.

As a result of using the suggested method, when the variable coefficients matrix is known, the task of the non-stationary system optimal control is reduced to the task of the equivalent stationary system optimal control for which solution methods are well-known and well processed.

Objective. Reducing energy intensity and improving the quality of products of various technological processes is an urgent task of the national economy of Ukraine.

Methods. To achieve this goal, we propose a method of modal synthesis of optimal stabilization laws using the method of uncertain coefficients, developed by the authors

Results. Algorithm of synthesis of the optimal controller in the absence and presence of delay in the control loop is developed. The method of selection and correction of the desired spectrum of roots is proposed. To eliminate self-oscillations in the presence of a delay in the control circuit, the R. Bass method is used.

Conclusions. The modal synthesis of optimal laws of stabilization of technological processes is proposed on the basis of the original method of uncertain coefficients. The complexity of the choice of the desired eigenvalues is overcome by the proposed procedure of construction and correction of the spectrum of roots in a closed system of optimal control. To eliminate the occurrence of stable self-oscillations (in the presence of a delay) in the stabilization process near a given trajectory, the Bass's method is proposed to be used. The simulation results confirm the correctness and effectiveness of the results.

KEYWORDS: technological process, linear-quadratic optimization task, AKOR method, modal synthesis, method of uncertain coefficients, choice and correction of roots spectrum, R. Bass's method.

ABBREVIATIONS

ACOR – analytic construction of the optimal regulators;

ACS – automatic control system.

NOMENCLATURE

$I(x,u)$ is a functional;

T is a the symbol of transposition;

t is a current time;

$\bar{u}$ is a vector of control actions;

p_i are the feedback coefficients;

λi is a roots of the characteristic equation;

i,j is a indexes;

a_{ij} are the coefficients of the matrix A;

b_i are the coefficients of the matrix B;

c_{ij} , f_i , d_i is a auxiliary variable;

col is a column vector;

k is a gain ratio;

$\tilde{x}$ is a extended state vector;

D is a determinant;

D_n is a determinant of dimension n x n;

D_{n+1} is a matrix with $(n+1)\times(n+1)$ coefficients and

$\tilde{pl}$ are column vectors with dimension (n+1);

ε is a real part of the complex root;

ξ is a degree of vibration damping;

φ is a phase shift;

ω is a circular frequency of oscillation;

μ is a some ratio;

$\bar{x}(t)$ is a state vector;

$u(t)$ is a scalar control;

θ is a delay in the control loop;

ω is a circular frequency;

f_i is a coefficient of the i-th open characteristic determinant.

A^* is a matrix of constant coefficients of dimensions (n+1)×(n+1);

B is a the column vector of dimension (n x 1);

$Q = \{q_{ij}\}$ is a diagonal matrix (n x n);

$H(\lambda)$ is a characteristic polynomial;

$q11$=$q22$= $q33$=1;

$\det(A + B_p^{-T} - I\lambda)$ is a the characteristic determinant of a closed optimal system.

INTRODUCTION

Systems synthesis task is one of the key tasks of both automatic control theory and practice. Its solution results

DOI 10.15588/1607-3274-2020-1-21

in definition of the structure of the automatic control system (ACS) and its parameters from the condition of the system sustainability and quality of transient processes (achieving the required performance, the inadmissibility of the considerable overshoot) improving control accuracy in steady-state conditions etc [1].

Linear controllers are an effective way to ensure dynamic performance of not only linear control objects of arbitrarily high order, but also of objects that contain non–linear and discrete units, which have a significant, but not a determining influence on dynamic processes.

One of the important classes of dynamic objects are various technological processes. Stabilization of technological processes is the basis for the development of optimal control systems. As the result of successful stabilization and remote manual control, it is possible to facilitate the withdrawal of equipment and machinery to open areas, which leads to a significant reduction in specific capital costs when creating new production capacities. The task of the regulators stabilizing the technological process is to counter the perturbation by the introduction of restorative effects. The problem of automation is especially acute for enterprises of chemical and petrochemical industry [2].

The majority of industrial controlled objects have delays. The presence of the delay is due to the final velocity of information flows propagation in the technological objects. The delay may also occur due to time spent on signal transmission or, as in happens more often, in can be caused by the phenomenon of simplifying assumptions, by virtue of which it is considered that action of intermediate and reinforcing links in the controlled object is reduced to a signal transmission with delay. In these cases it is called transport delay systems [3].

Inertia of the operator himself has a significant impact on the management quality in addition to the delay in the signal transmission. Therefore, it's imperative to have optimal (reference) dynamic implementation (control laws) in preparation of the operator taking into account the inertia and delay in the control loop.

In this article authors propose a procedure for the synthesis of the optimal modal law stabilization of linear stationary systems with delay based on the method of undetermined coefficients, which is proposed by the authors below.

1 PROBLEM STATEMENT

Let the dynamics of the process have the form:

$$\dot{\bar{x}}(t) = A\bar{x}(t) + Bu(t-\theta), \tag{1}$$

Boundary conditions:

The most common for the stabilization of technological processes is a quadratic criterion of shape quality:

$$I(x,u) = \int_0^\infty \left[\bar{x}(t)^T Q\bar{x}(t) + u^2(t)\right]dt\,. \tag{2}$$

The choice of the quality criterion (2) is due to the fact that it reflects the accuracy of tracking the normative indicators of technological processes and energy consumption for the stabilization process.

The General statement of the problem of stabilization of technological processes is as follows:

– it is necessary to find a control that translates the system (1) from an arbitrary initial state to a zero finite state and minimizes the quality criterion (2).

2 REVIEW OF THE LITERATURE

There are two main deterministic approaches to create the control system for the object's state vector – analytical design of optimal controllers and modal control.

Professor A. M. Letov [4] published his work in 1960, in which the analytical solution of the problem of linear stationary object's optimal stabilization with a quadratic quality functional was obtained, it was later called "analytic construction of the optimal regulators" (ACOR).

Problem of linear non-stationary objects optimization is also solved in Kalman's work [5] published in 1960.

ACOR has the ultimate goal of obtaining control law purely analytically, based on the requirements for management quality.

Synthesis of the desired optimal closed loop control system using ACOR depends on the designer choice of suitable coefficient values of quality criterion is not quite convenient because of absence of obvious relationship between selected coefficients and transients in a closed–loop system.

In addition, the application of the ACOR method leads to the necessity of solving nonlinear matrix Riccati equation, which is a non-trivial task and requires the use of special numerical procedures [6].

The essence of the modal synthesis of optimal control is to determine the numerical values of the delayless feedback transmission coefficients in all the variables of the technological processes state in order to ensure a predetermined distribution of the characteristic equation roots (eigenvalues) in the closed-loop control system [7].

For optimal stabilization of the technological processes proposed modal synthesis using the method of uncertain coefficients. Let us first consider the case when there is no delay in the control loop.

3 MATERIALS AND METHODS

It is known [6] that for systems (1)in the case of a quadratic quality criterion (2), extreme control is a linear function of state variables:

$$\bar{u} = p^{-T}\bar{x}. \tag{3}$$

Moreover, if the vector of feedback coefficients is chosen in such a way that the poles of the closed system (1) are located at preassigned arbitrary points, then the required dynamic properties will be provided in the closed system [4]. Thus, this problem is reduced to the choice of the optimal location of the poles and determination of the feedback coefficients.

We prove the following statement.

DOI 10.15588/1607-3274-2020-1-21

Statement. We show that the unknown coefficients of the characteristic determinant of a closed optimal system [7]:

$$\det(\lambda) = \left|A + Bp^{-T} - I\lambda\right| = \begin{vmatrix} a_{11} + b_1 p_1 - \lambda \cdots a_{1j} p_j \cdots a_{1n} + b_1 p_n \\ a_{j1} + b_j p_1 \cdots a_{jj} + b_j p_j - \lambda \cdots a_{jn} + b_j p_n \\ a_{n1} + b_n p_1 \cdots a_{nj} + b_n p_j \cdots a_{nn} + b_n p_n - \lambda \end{vmatrix}.$$

linearly enter into the expression for the coefficients of the characteristic polynomial of a closed system.

Proof. Indeed, let's suppose that. Then, subtracting the *k*-th line from the j th line, multiplied by we get a determinant equal to the original, in which the feedback coefficients enter the k th line. Expanding it along this line and grouping the terms with the corresponding powers, we finally arrive at the following expression of the characteristic polynomial of the closed system (4a) or (4b):

$$H(\lambda) = \lambda^n + \left(\sum_{i=1}^{n} c_{n-1,i} p_i + d_{n-1}\right)\lambda^{n-1} + \left(\sum_{i=1}^{n} c_{0,i} p_i + d_0\right); \quad (4a)$$

$$H(\lambda) = \lambda^n + \left(\bar{c}_{n-1}^{T} p + d_{n-1}\right)\lambda^{n-1} + \ldots + \left(\bar{c}_0^{T} \bar{p} + d_0\right). \quad (4b)$$

We define the unknown parameters c_{ji} and $d_i (j = \overline{0, n-1}; i = \overline{1, n})$, in n+1 n+1 step using the undetermined coefficients method. To do this, we put $p_i = 0 (i = \overline{1, n})$ in the characteristic determinant at the first step and reveal it by one of the known numerical methods and find that the coefficients found for different powers of λ determine the unknown coefficients $d_j (i = \overline{0, n-1})$ in the expressions for the characteristic polynomial of the closed system for the corresponding powers of λ. In the next n steps, setting sequentially one of the coefficients $p_i (i = \overline{1, n})$ equal to one while others remain zero and revealing the characteristic determinant, we obtain expressions for the unknown parameter c_{ji}, $\lambda^j (j = \overline{0, n-1})$ or the corresponding power $\lambda^j (j = \overline{0, n-1})$ in the characteristic polynomial of the closed system.

$$c_{ji} = f_i - d_i. \quad (5)$$

On the other hand, the characteristic polynomial of a closed system with the desired roots $\lambda_1, \lambda_2, ..., \lambda_n$ has the form [7]

$$F(\lambda) \prod_{i=1}^{n} (\lambda - \lambda_i) = \sum_{j=0}^{n-1} 1_j \lambda^j + \lambda^n. \quad (6)$$

As a result, to determine the feedback coefficients pi in expression (2), we equate the expressions for the coefficients for the same powers in (4) and (6) and obtain a system of linear algebraic equations:

$$col\left(\bar{c}^{T}, \bar{c}^{T}, ..., \bar{c}^{T}\right)\bar{p} = \bar{1} - \bar{d}, \quad (7)$$

where

$$\bar{1} = (1_{n-1}, 1_{n-1}, ..., 1_0), \bar{d} = (d_{n-1}, d_{n-2}, ..., d_0)\, y.$$

Now consider the procedure for modal synthesis based on the undefined coefficients method proposed for linear dynamical systems with transport delay [5, 6].

Let the dynamics model (1) of the technological process is described as

$$\dot{\bar{x}} = A\bar{x} + By, \quad (8)$$

where $\bar{x} = (x_1, x_2, ..., x_n)^T$ is fully measured vector of system states deviation from a predetermined trajectory of movement; A,B is a coefficient matrix with dimension $n \times n$, $n \times 1$; y is a scalar, characterized by deviation of controls, taking into account the reaction of the operator, the dynamic model has the form

$$\dot{y} = \lambda_y y + d_u u(t - \theta), \quad (9)$$

where λ_y, d_u, θ are constants determined by psychophysical features of operators (and besides $\lambda_y = -\frac{1}{T}; d_u = \frac{k}{T}$ $u(t)$ is a scalar control action, which will be sought in the form (2). The objective is to determine the coefficients $\bar{p} = (p_1, p_2, ... p_n)^T$, providing some predetermined dynamic characteristics of the stabilization process and achieving sustainable programmed movement of the system (8).

As the operator delay θ is sufficiently small value, we'll write the equation (9) as a

$$\dot{y}(t) = \lambda_y y(t) + d_u u(t) - d_u \theta \dot{u}(t). \quad (10)$$

In that case if in some way estimate or measure the condition of the operator $y(t)$, the system (8), (10) is fully observed and the problem is solved as follows.

We take into consideration the advanced phase vector. Then the closing equation has the form

$$\tilde{x} = (x_1, x_2, ..., x_n, x_{n+1} = y)^T.$$

$$u = p^T \tilde{x}, \quad (11)$$

and the characteristic polynomial of the closed-loop system (8), (10) takes the form:

DOI 10.15588/1607-3274-2020-1-21

$$\det(A^* - I\lambda) = \begin{vmatrix} \dfrac{A - I\lambda}{d_u\left(\bar{p}^T - \theta\bar{p}^T A\right)} & \dfrac{B}{\lambda_y + d_u p_{n+1} - \theta\bar{p}^T B - \lambda} \\ \dfrac{}{1 + d_u\theta \quad p_{n+1}} & \dfrac{}{1 + d_n\theta \quad p_{n+1}} \end{vmatrix} = 0, \quad (12)$$

where A^* is a matrix

$$(n+1)\times(n+1), \bar{p} = (p_1, p_2, \ldots p_n)^T,$$
$$\Delta_{11} = \Delta_{12} = \Delta_{21} = \Delta_{22}.$$

The multiplication of all the elements of a row or column by the factor μ is equivalent to multiplying the determinant on μ [7]. Hence, the determinant (12) can be written and therefore assuming that the, we'll put

$$\begin{vmatrix} \dfrac{A - I\lambda}{\bar{p}^T - \theta\bar{p}^T A} & \dfrac{B}{\lambda_y + d_u p_{n+1} - d_u\theta\bar{p}^T B - \lambda(1 + d_u\theta p_{n+1})} \end{vmatrix} = 0. \quad (13)$$

It is easy to show that the determinant (13) is a polynomial of degree (n+1) on λ, and its coefficients are linearly dependent on , i.e.

$$\det(A^* - I\lambda) = H(\lambda, \bar{p}) = \lambda^{n+1} + (\bar{d}_n^T\bar{p} + d_n^0)\lambda^n + \ldots + (\bar{d}_n^T\bar{p} + d_n^0) = 0. \quad (14)$$

Indeed, when uncovering the determinant (13) in the last line, in which each element is a linear combination of the coefficients *p*, we're getting the expression (14).

Determination of unknown coefficients $d_i, d_i^0 (i = \overline{0,n})$ is made similarly to the procedure cited in this paper above. When equating between the coefficients of the polynomial powers (14) and the polynomial with spectrum $\{\lambda_i\}\left(i = \overline{1, n+1}\right)$ selected to provide specified quality parameters of transient processes

$$L(\lambda) = \prod_{i+1}^{k+1}(\lambda - \lambda_i) = \sum_{k=0}^{n+1} 1_k \lambda^k, \quad (15)$$

where $l_{n+1} = 1$, we get the joint system of linear algebraic equations

$$D_{n+1} p = \tilde{l}. \quad (16)$$

The solution of system (16) provides the defined spectrum $\{\lambda_i\}(i = \overline{1, n+1})$ to a closed-loop system. Frequently it is not possible to evaluate or measure the state of the operator *y*(*t*) in real conditions. Then it is necessary to put $p_n + 1 \equiv 0$ in the closing equation (11). As a result, the characteristic determinant of a closed-loop system has the form.

$$\det(A^* - I\lambda) = \begin{vmatrix} \dfrac{A - I\lambda}{d_u(\bar{p}^T - \theta\bar{p}^T A)} & \dfrac{B}{\lambda_y - d_u\theta\bar{p}^T B - \lambda} \end{vmatrix}. \quad (17)$$

Desired characteristic polynomial is determined, as in the previous case, by the expression (15). When equating the coefficients of the polynomials (17) and (15) with the same powers λ we obtain incompatible systems of linear algebraic equations in contrast to (16)

$$D_n \bar{p} = \tilde{l}. \quad (18)$$

It is possible to use the least squares method [8] for solving such a system, according to which the vector of unknown coefficients $\bar{p}$ is approximately defined as

$$\bar{p} = (D_n^T D_n)^{-1} D_n \tilde{l}. \quad (19)$$

The optimal stabilization law (11) of the system (1), synthesized, proposed by the method of indefinite coefficients, provides the given dynamic properties of the process of stabilization of the system in the event of deviations from the given (software) trajectory of motion. However, this law does not eliminate the occurrence due to the presence of a lag of stable self-oscillations at the end point of the stabilization process near the given trajectory of motion. To compensate for the delay, a modified Bass's method [8] proposed, the essence of which is as follows. The delay compensation method [8] to eliminate this effect, according to which it is necessary to find a surface spaced in delay time from the zero error point lying on the trajectory of the motion program (1) by integrating system (1) in reverse time. In fact, this surface is a tube inside which the programmed trajectory is located.

To ensure the specified dynamic parameters of transient processes in the stabilization of the technological processes below the proposed methodology for the selection and correction of the spectrum of the roots.

Usually in stabilization mode technological processes management quality is defined by transition process time tn.n. and a range of this process simplification

$$\xi = \frac{x_j(t_{n.n})}{x_j(t_0)} < 1, \quad j = \overline{1, n.} \quad (20)$$

If $\lambda_0 = \varepsilon_0 + i\omega_0$ is a dominant root then solution of system (1) can be approximately written in the form

$$x_j = x_j(t_0)e^{\varepsilon_0 i} \cos(\omega_0 t + j_i), \quad j = \overline{1, n.} \quad (21)$$

From equation (21) based on expression (20) we obtain

$$\frac{x_j(t_{n.n})}{x_j(t_0)} \le e^{\varepsilon_0 t_{n.n}} \le \xi, \quad (22)$$

where

DOI 10.15588/1607-3274-2020-1-21

$$\varepsilon_0 \le \frac{\ln \xi}{t_{n.n}} < 0.$$

We choose such value of the imaginary part that is equal l/tn.n. Variable *xj*(*t*) will make one oscillation around the equilibrium position at the same time during the transition process and will strive for it from the opposite side relative to the initial disturbance, which is highly desirable for physical reasons.

In order to avoid overshooting the remaining roots of the characteristic polynomial should be placed as close as possible to the dominant with implementation of such conditions

$$\begin{aligned} &\omega_0 < \omega_1 < \omega_2 < ..., \\ &|\varepsilon_0| < |\varepsilon_1| < |\varepsilon_2 < ...,| \end{aligned}, \qquad (23)$$

so that components with the large fluctuations will dump more rapidly

$$|\lambda_k| - |\lambda_{k-1}| > 0{,}1(|\lambda_k|), \qquad (24)$$

and that the roots are not merged into multiples. It is desirable to have roots on the complex plane as much as possible to the left in order to reduce transition time. However, constraints on state variables impose certain restrictions on the roots modules too.

Given the notation (21) we write

$$\dot{x}_j = \sqrt{\omega^2 + \varepsilon^2}\, x(t_0) e^{\varepsilon t} \cos(\omega t + \varphi_j). \qquad (25)$$

Each *j*-th equation of system (22) generates two upper limits of the roots modules in the characteristic polynomial, due to by the same restriction on the left and right sides of the *j*-th equation of system (22).

Taking into account the expression (25) we define that for the left side of the *j*-th equation of system (7)

$$\max_t \max_\lambda x_j = \max \sqrt{\omega^2 + \varepsilon^2}\, x_j(t_0). \qquad (26)$$

And for the right side

$$\max_t \max_\lambda \sum_{i=1}^{n} a_{ji} x_j \le \sum_{i=1}^{n} |a_{ji} x_i(t_0)|. \qquad (27)$$

Comparing the expressions (26) and (27), in the absence of an explicit dependence of inequality (27) from the roots module the following inequality can be written as:

$$\max_\lambda \sqrt{\omega^2 + \varepsilon^2} \le \frac{\sum_{i=1}^{n} |a_{jl} x_i(t_0)|}{x_j(t_0)}. \qquad (28)$$

DOI 10.15588/1607-3274-2020-1-21

The most severe restriction of (28) will give us the left edge of the characteristic polynomial root distribution. Thus, the increasing ε in order to accelerate the decay process results in minimization ω considering expressions (23) and (24). Roots location corrected after the transient modeling, based on the superimposed state variables limits by changing the characteristic polynomial coefficients.

Let's suppose that the j-th state variable is constrained by $\max |x_j| \le x_j^{pres}$. In this case, we homothetically shift all roots relative to the origin (according to Vieta's theorem) with the homothetic coefficient by multiplying coefficients of the characteristic polynomial of degree 1 by the value $\left[\frac{x_j^{pres}}{x_j}\right]$ [9].

Also, the value of $\max|x_j|$ will change according to the expression (21).

4 EXPERIMENTS

We will carry out modeling for two types of technological processes, dynamic models of which are most common in practice. The aim of the simulation is a comparative analysis of the transients obtained by the standard ACOR method and modal synthesis based on the method of uncertain coefficients.

Technological process 1. Let the dynamics of the technological process described by a system of equations of the form:

$$\frac{dx_1}{dt} = x_2; \quad \frac{dx_2}{dt} = a_{22}x_2 + b_2 u.: \qquad a_{22} = 1; \ b_2 = 1.$$

Thus, the control object is a serial connection of the integrating and aperiodic links. It is necessary to define a control law that provides a minimum of the functional (2).

Boundary conditions:

$$x_1(0) = x_{10}, \ \ x_2(0) = x_{20}; \ \ x_1(\infty) = x_2(\infty) = 0.$$

We consider two cases: a) x_{10}=1; x_{20}=0; b) x_{10}=5; x_{20}=0;

On the Fig. 1 graphics of transients of stabilizing for cases a), b) obtained by ACOR and modal synthesis, , is shown.

Technological process 2. Now let's suppose that the dynamics of the technological process is described by a system of equations of the form:

$$\dot{\bar{x}}(t) = A\bar{x}(t) + Bu(t), \bar{x}(t),$$

where $\bar{x}(t) = (x1(t), x2(t), x3(t))$T-state vector; $u(t)$ – a scalar control.

We assume that the delay in the control loop is missing.

Let's also assume that $A = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

For the stabilization of technological process a quadratic criterion of shape quality (2) is used,

We consider two cases: a) $x_{10}=1$; $x_{20}=0$; $x_{30}=0$;

b) $x_{10}=5$; $x_{20}=0$; $x_{30}=0$,

5 RESULTS

On the Fig. 1 shows graphics of transients of stabilizing for cases a and b obtained by ACOR and modal synthesis for the technological process 1.

On the Fig. 2 graphics of transients of stabilizing for cases a and b obtained by ACOR and modal synthesis for the technological process 2.

6 DISCUSSION

From these graphics (Fig. 1 and Fig. 2) we can see that from the point of view of modal synthesis, providing the given dynamic parameters of the transient stabilization processes is more effective. On the Fig. 1 it concerns the energy saving component. On the Fig. 3 it concerns to the accuracy of tracking the required stabilization parameter values. With the help of the proposed modal synthesis based on the method of uncertain coefficients, it is possible to ensure the performance of such dynamic indicators of the quality of transients as: stabilization time, overshoot, simplification, degree of oscillation, etc. This is the main advantage of this method over the ACOR method, since the latter does not have a direct relationship between the coefficients of the quality criterion and the feedback coefficients. In addition, as shown above, the method works in the presence of a small delay in the control loop.

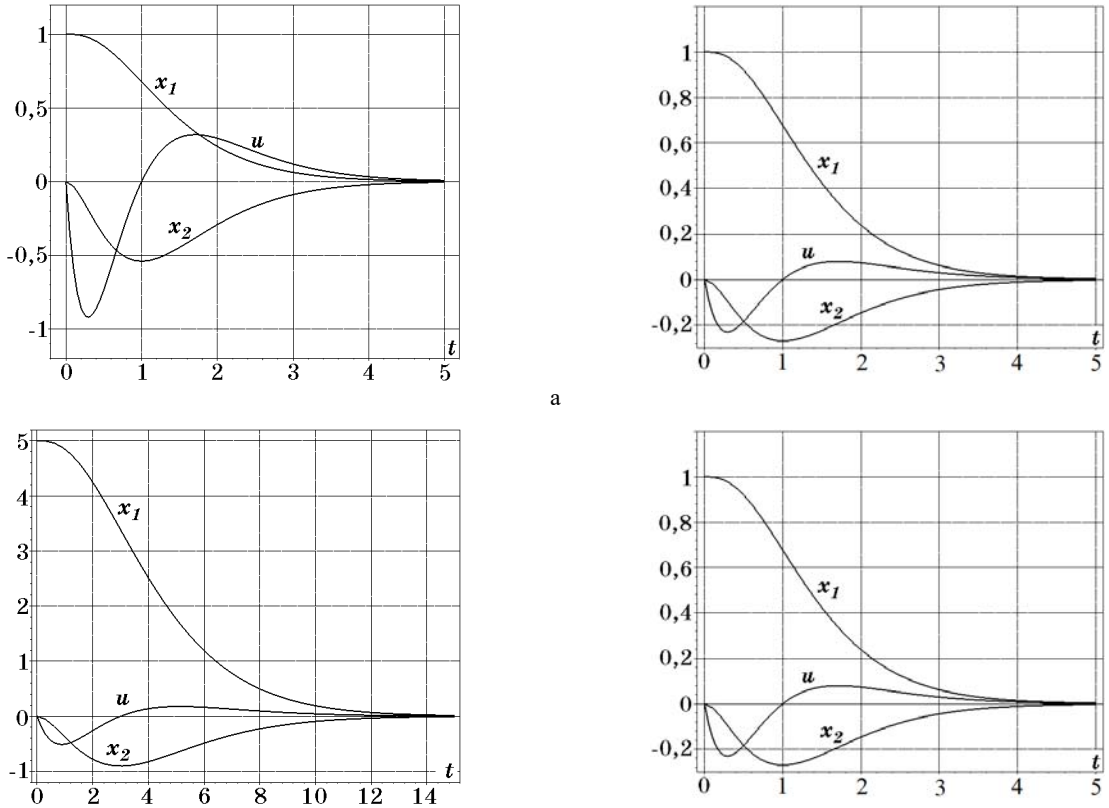
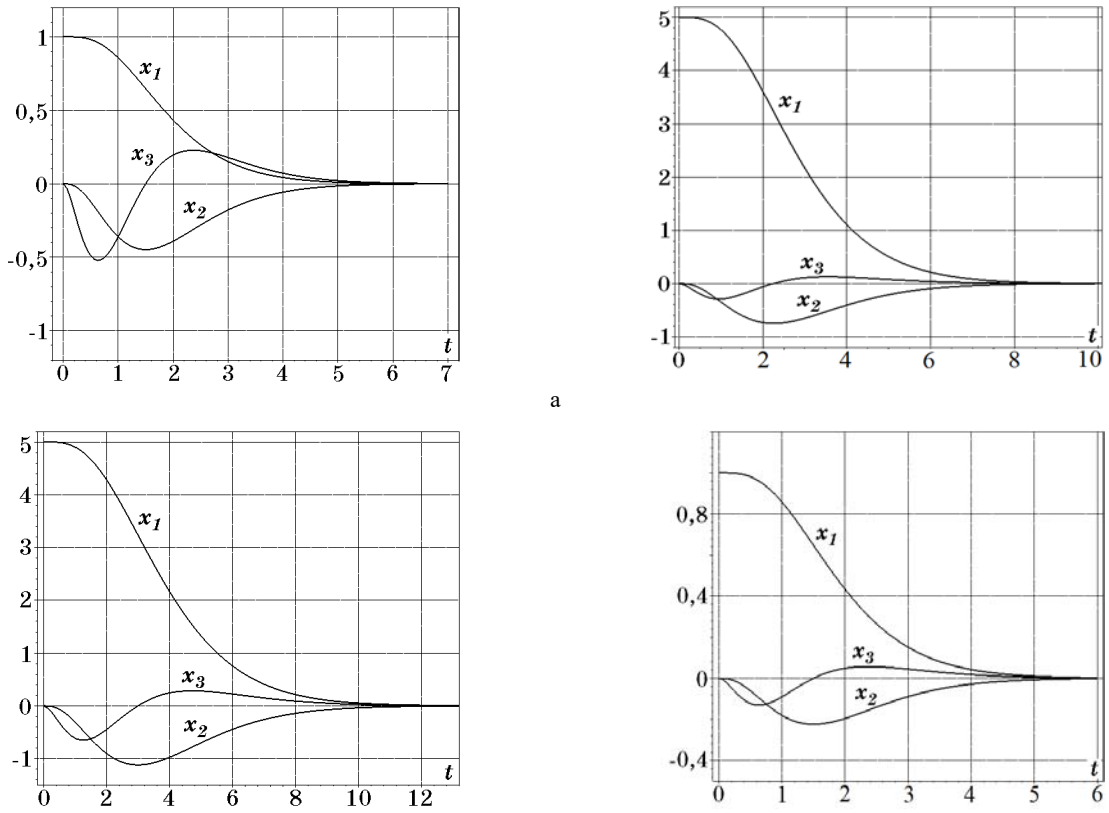


Figure 1 – Transient graphics obtained by ACOR (left) and modal synthesis (right)

DOI 10.15588/1607-3274-2020-1-21



a

b

Figure 2 – Transient graphics obtained by ACOR (left) and modal synthesis (right)

CONCLUSIONS

The modal synthesis of linear closed stationary systems with the optimal control law (3) proposed in the article can provide the required dynamic properties in technological processes according to the given parameters. The procedure of modal synthesis of the optimal control law carries out on the method of uncertain coefficients proposed in the article. The difficulty of choosing the required eigenvalues overcomes the suggested procedure, construction and correction of the spectrum of roots of the closed-loop optimal control system of technological processes. Synthesis of closed-loop optimal control systems is generalized to incompletely observed processes and processes with delay in the control loop. In addition, the proposed procedure of modal synthesis can be used for one class of non-stationary systems, for which the method of equivalent transformation proposed in [10] is valid. The simulation results confirm the correctness and effectiveness of the received results.

REFERENCES

1. Pupkov K. A., Egupov N. D. Methods of classical and modern theory of automatic control, *Theory of optimization of automatic control systems.* Moscow, The Bauman University Publishing House, 2004, Vol. 4, 744 p.
2. Malyshkin A. B. Problems and prospects of automation of technological processes at petrochemical enterprises [Electronic resource]. Access mode: DOI: 10.18454/IRJ.2016.47.097.
3. Yanushevsky R. T. Management of objects with delay. Moscow, Nauka, 1978, 410 p.
4. Letov F. A. Analytical Design of Controllers/ Letov // *Automation and telemechanics*, 1960, No. 4, pp. 436–441. No. 5, pp. 561–568. No. 6, pp. 661–665. 1961, No. 4, pp. 425–435.
5. Kalman R. E. Contribution to the theory of optimal control, *Bulletin of the society of Mechanics and Mathematicians*, 1960, Vol. 12, No. 2, pp. 102–119.
6. Bystrov S. V., Grigoriev V. V., Pershin I. M. et al. The Synthesis of linear-quadratic control laws for continuous-time dynamic objects, *International research journal of St. Petersburg State University,* 2017, No. 2(56), pp. 97–100 DOI: https://doi.org/10.23670/IRJ.2017.56.052
7. Athans M., Falb P. L. Optimal Control: An Introduction to the Theory and Its Applications. North Chelmsford, Courier Corporation, 2013, 879 p.
8. Bass R. W. Improved on-off Missile Stabilization, *Jet Propulsion,* 1956, Vol.26, pp. 415–417.
9. Andreev Yu. N. Control of Finite-Dimensional Linear Objects. Moscow, Nauka, 1976, 424 p.
10. Melkumyan E. Yu., Soldatova M. A. Method of the equivalent conversion of one class of linear nonstationary systems, *Adaptive Systems of Automatic Control Inter-Branch Scientific and technological Digest,* 2015, Issue 1(26), pp. 102–105. https://doi.org/10.20535/15608956.26.2015.45515

Received 25.09.2019.
Accepted 29.12.2019.

DOI 10.15588/1607-3274-2020-1-21

УДК 621.51

МЕТОД НЕВИЗНАЧЕНИХ КОЕФІЦІЄНТІВ У ЗАВДАННЯХ ОПТИМАЛЬНОЇ СТАБІЛІЗАЦІЇ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

Стенін О. А. – д-р техн. наук, професор кафедри технічної кібернетики, Київський політехнічний інститут ім. Ігоря Сікорського, Київ, Україна.

Дроздович І. Г. – канд. техн. наук, ст. науковий співробітник, Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ, Україна.

Солдатова М. О. – ст. викладач кафедри автоматизованих систем обробки інформації та управління, Київський політехнічний інститут ім. Игоря Сикорского, Київ, Україна.

АНОТАЦІЯ

Актуальність В даній статті розглядається метод еквівалентного перетворення, зміст якого полягає в заміні деякого класу нестаціонарних систем стаціонарними, для яких методи оптимізації добре опрацьовані. Актуальність методу обумовлена тим, що у більшості методів оптимального управління, які розроблені для неперервних систем, задачі розглядаються у часовому просторі з використанням простору станів та теорії матриць. Відомо, що всі реальні об'єкти управління в той чи іншій мірі є нелінійними та нестаціонарними. Аналіз та синтез систем управління для таких об'єктів представляє собою складну математичну проблему, рішення якої до теперішнього часу отримано для деяких окремих випадків.

В результаті використання запропонованого методу, коли відома матриця змінних коефіцієнтів, задача оптимального управління нестаціонарною системою зводиться до рішення задачі оптимального управління еквівалентною стаціонарною системою, методи рішення якої достатньо відомі та добре опрацьовані.

Метод. Для досягнення поставленої мети запропоновано метод модального синтезу оптимальних законів стабілізації з використанням розробленого авторами методу невизначених коефіцієнтів

Результат. Розроблено алгоритм синтезу оптимального регулятора у випадках відсутності і наявності запізнювання в контурі управління. Запропонована методика вибору і корекції бажаного спектру коренів. Для усунення автоколивань при наявності запізнювання в контурі управління використовується метод Р. Бесса.

Висновок Запропоновано модальний синтез оптимальних законів стабілізації технологічних процесів на основі оригінального методу невизначених коефіцієнтів. Складність вибору шуканих власних значень долається запропонованою процедурою побудови і корекції спектру коренів в замкнутій системі оптимального управління. Для виключення виникнення стійких автоколивань (при наявності затримки) в процесі стабілізації поблизу заданої траєкторії пропонується використовувати метод Бесса. Результати моделювання підтверджують коректність і ефективність отриманих результатів.

КЛЮЧОВІ СЛОВА технологічний процес, лінійно-квадратична задача оптимізації, метод АКОР, модальний синтез, метод невизначених коефіцієнтів, вибір і корекція спектру коренів, метод Р. Бесса.

УДК 621.51

МЕТОД НЕОПРЕДЕЛЕННЫХ КОЭФФИЦИЕНТОВ В ЗАДАЧАХ ОПТИМАЛЬНОЙ СТАБИЛИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Стенин А. А. – д-р техн. наук, профессор кафедры технической кибернетики, Киевский политехнический институт им. Игоря Сикорского, Киев, Украина.

Дроздович И. Г. – канд. техн. наук, ст. научный сотрудник, Институт телекоммуникаций и глобального информационного пространства НАН Украины, Киев, Украина.

Солдатова М. А. – ст. преподаватель кафедры автоматизированных систем обработки информации и управления, Киевский политехнический институт им. Игоря Сикорского, Киев, Украина.

АННОТАЦИЯ

Актуальность. В данной статье рассматривается метод эквивалентного преобразования, смысл которого заключается в замене некоторого класса нестационарных систем стационарными, для которых методы оптимизации хорошо проработаны. Актуальность метода обусловлена тем, что в большинстве методов оптимального управления, разработанные для непрерывных систем, задачи рассматриваются во временном пространстве с использованием пространства состояний и теории матриц. Известно, что все реальные объекты управления в той или иной степени являются нелинейными и нестационарными. Анализ и синтез систем управления для таких объектов представляет собой сложную математическую проблему, решение которой до настоящего времени получено для некоторых частных случаев.

В результате использования предложенного метода, когда известна матрица переменных коэффициентов, задача оптимального управления нестационарной системой сводится к решению задачи оптимального управления эквивалентной стационарной системою, методы решения которой достаточно известные и хорошо проработанные.

Метод. Для достижения поставленной цели предложен метод модального синтеза оптимальных законов стабилизации с использованием разработанного авторами метода неопределенных коэффициентов.

Результаты. Разработан алгоритм синтеза оптимального регулятора в случаях отсутствия и наличия запаздывания в контуре управления. Предложена методика выбора и коррекции желаемого спектра корней. Для устранения автоколебаний при наличии запаздывания в контуре управления используется метод Р. Бэсса.

Выводы. Предложен модальный синтез оптимальных законов стабилизации технологических процессов на основе оригинального метода неопределенных коэффициентов. Сложность выбора искомых собственных значений преодолевается предложенной процедурой построения и коррекции спектра корней в замкнутой системе оптимального управления. Для

DOI 10.15588/1607-3274-2020-1-21

исключения возникновения устойчивых автоколебаний (при наличии задержки) в процессе стабилизации вблизи заданной траектории предлагается использовать метод Бэсса. Результаты моделирования подтверждают корректность и эффективность полученных результатов.

КЛЮЧЕВЫЕ СЛОВА: технологический процесс, линейно-квадратичная задача оптимизации, метод АКОР, модальный синтез, метод неопределенных коэффициентов, выбор и коррекция спектра корней, метод Р. Бэсса.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Пупков К. А., Єгупов Н. Д. Методи класичної та сучасної теорії автоматичного управління / К. А. Пупков, Н. Д. Єгупов // Теорія оптимізації автоматичних систем управління. – М .: Видавництво університету Баумана, 2004. – Вип. 4 – 744 с.
2. Малишкін А. Б. Проблеми та перспективи автоматизації технологічних процесів на нафтохімічних підприємствах [Електронний ресурс] / Малишкін А. Б. – Режим доступу: DOI: 10.18454 / IRJ.2016.47.097.
3. Янушевський Р. Т. Управління об’єктами із запізненням / Р. Т. Янушевський. – М .: Наука, 1978. – 410 с.
4. Ф. Летов А. Аналітичне проектування контролерів / Летов // Автоматизація та телемеханіка. – 1960. – №4. – С. 436–441, № 5. – С. 561–568, № 6. – С. 661–665, 1961. – № 4. – С. 425–435.
5. Kalman R. E. Contribution to the theory of optimal control / R. E. Kalman // Bulletin of the society of Mechanics and Mathematicians. – 1960. – Vol. 12, № 2. – P. 102–119.
6. Синтез законів лінійно-квадратичного управління для динамічних об’єктів безперервного часу / [С. В. Бистрова, В. В. Григор’єва, І. М. Першина та ін.] // Міжнародний науковий журнал Петербурзького державного університету. – 2017.– № 2 (56). – С. 97–100. DOI: https://doi.org/10.23670/IRJ.2017.56.052
7. AthansOptimal Control: An Introduction to the Theory and Its Applications / M. Athans, P. L. Falb. – North Chelmsford : Courier Corporation, 2013 – 879 p.
8. Bass R. W. Improved on-off Missile Stabilization / R. W. Bass // Jet Propulsion. – 1956. – Vol. 26. – P. 415–417.
9. Андрєєв Ю. Н. Контроль кінцевомірних лінійних об’єктів / Ю. Н. Андрєєва. – М. : Наука, 1976. – 424 с.
10. Мелкумян Е. Ю. Метод еквівалентного перетворення одного класу лінійних нестаціонарних систем / Є. Ю. Мелкумян, М. А. Солдатова // Адаптивні системи автоматичного управління міжгалузевим науково-технічним дайджестом. – 2015. – Випуск 1 (26). – С. 102–105. https://doi.org/10.20535/15608956.26.2015.45515

DOI 10.15588/1607-3274-2020-1-21

Наукове видання

Радіоелектроніка,

інформатика,

управління

№ 1/2020

Науковий журнал

Головний редактор – д-р техн. наук С. О. Субботін

Заст. головного редактора – д-р техн. наук Д. М. Піза

Комп’ютерне моделювання та верстання С. В. Зуб
Редактор англійських текстів С. О. Субботін

Оригінал-макет підготовлено у редакційно-видавничому відділі НУ «Запорізька політехніка»

Свідоцтво про державну реєстрацію
КВ № 24220-14060 ПР від 19.11.2019.

Підписано до друку 14.05.2020. Формат 60×84/8.
Папір офс. Різогр. друк. Ум. друк. арк. 25,34.
Тираж 300 прим. Зам. № 529.

69063, м. Запоріжжя, НУ «Запорізька політехніка», друкарня, вул. Жуковського, 64

Свідоцтво суб’єкта видавничої справи
ДК № 6952 від 22.10.2019.